



Network and Security Manager

Configuring Secure Access Devices Guide

Release
2012.2



Published: 2013-01-03
Revision 01

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986-1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Network and Security Manager Configuring Secure Access Devices Guide

Release 2012.2

Copyright © 2013, Juniper Networks, Inc.

All rights reserved.

Revision History

January 2013 —01

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

	About This Guide	ix
	Objectives	ix
	Audience	ix
	Document Conventions	ix
	List of Technical Publications	xi
	Requesting Technical Support	xii
	Self-Help Online Tools and Resources	xii
	Opening a Case with JTAC	xii
Part 1	Getting Started	
Chapter 1	Understanding Secure Access Device Configuration	3
	NSM and Secure Access Device Management Overview	3
	Communication Between a Secure Access Device and NSM Overview	3
	Secure Access Device Services and Device Configurations Supported in NSM	5
Chapter 2	Secure Access Device and NSM Installation Overview	7
	Secure Access Device Installation Overview	7
	NSM Installation Overview	7
Part 2	Integrating Secure Access Devices	
Chapter 3	Adding Secure Access Devices	11
	Importing a Secure Access Device	11
	Installing and Configuring a Secure Access Device	11
	Adding a Secure Access Device Through NSM	12
	Configuring and Activating the NSM agent on the Secure Access Device	13
	Confirming Connectivity and Importing the Secure Access Device Configuration	14
	Requirements for Importing a Secure Access Device into NSM Through a Reachable Workflow	14
	Adding a Secure Access Device Through a Reachable Workflow	15
	Importing Multiple Secure Access Devices	16
	Creating the CSV File	16
	Validating the CSV File	17
	Adding and Importing Multiple Secure Access Devices	18
	Verifying Imported Device Configurations	19
	Using Device Monitor	19
	Using Device Manager	19
	Using Job Manager	20
	Using Configuration Summaries	20

Chapter 4	Adding Secure Access Clusters	23
	Adding a Secure Access Cluster Overview	23
	Adding a Secure Access Cluster with Imported Cluster Members	24
	Installing and Configuring the Cluster	25
	Adding the Cluster in NSM	25
	Adding the Cluster Members in NSM	25
	Configuring and Activating the DMI Agent on the Cluster	27
	Importing Cluster Configuration	27
Chapter 5	Working with Secure Access Templates	29
	Creating and Applying a Secure Access Device Template	29
	Creating the Template	29
	Applying the Template	30
	Promoting a Secure Access Device Configuration to a Template	31
Part 3	Configuring Secure Access Devices	
Chapter 6	Configuring User Roles and Administrator Roles	35
	Configuring Secure Access Device User Roles (NSM Procedure)	35
	Creating Secure Access Role-Based Source IP Alias (NSM Procedure)	38
	Configuring Secure Access General Session Options (NSM Procedure)	39
	Creating and Configuring Secure Access Device Administrator Roles (NSM Procedure)	43
Chapter 7	Configuring Terminal Services Using Remote Access Mechanism	51
	Terminal Services Overview	51
	Configuring Terminal Services on a Secure Access Device User Role (NSM Procedure)	52
	Terminal Services User Experience	61
	Terminal Services Execution	62
Chapter 8	Configuring Access Options using Remote Access Mechanisms	65
	Configuring Access Options using Remote Access Mechanisms Overview	65
	Configuring File Rewriting on a Secure Access Device User Role (NSM Procedure)	66
	Configuring Network Connect on a Secure Access Device User Role (NSM Procedure)	69
	Configuring Secure Application Manager on a Secure Access Device User Role (NSM Procedure)	73
	Configuring Secure Meeting on a Secure Access Device User Role (NSM Procedure)	78
	Configuring Web Rewriting on a Secure Access Device User Role (NSM Procedure)	84
	Configuring Telnet/SSH on a Secure Access Device User Role (NSM Procedure)	89
Chapter 9	Configuring Secure Access Resource Profiles	93
	Configuring a JSAM Resource Profile (NSM Procedure)	93
	Configuring a Citrix Terminal Services (Custom ICA) Resource Profile (NSM Procedure)	95

	Configuring a Citrix Terminal Services (Default ICA) Resource Profile (NSM Procedure)	99
	Configuring a Citrix Listed Application Resource Profile (NSM Procedure)	104
	Configuring Citrix Web Applications Resource Profile (NSM Procedure)	110
	Configuring Custom Web Applications Resource Profile (NSM Procedure)	112
	Configuring File Rewriting Resource Profiles (NSM Procedure)	120
	Configuring Windows Terminal Services (NSM Procedure)	124
	Configuring a Telnet/SSH Resource Profile (NSM Procedure)	129
	Configuring WSAM Resource Profile (NSM Procedure)	131
	Configuring Bookmarks for Virtual Desktop Resource Profiles (NSM Procedure)	134
Chapter 10	Configuring Secure Access Resource Policies	137
	Configuring a File Rewriting Resource Policy (NSM Procedure)	137
	Configuring a Secure Application Manager Resource Policy (NSM Procedure)	143
	Configuring a Telnet and Secure Shell Resource Policy (NSM Procedure)	146
	Configuring a Terminal Service Resource Policy (NSM Procedure)	148
	Configuring Web Rewriting Resource Policies (NSM Procedure)	151
	Configuring a Network Connect Connection Profile Resource Policy (NSM Procedure)	155
	Defining Network Connect Split Tunneling Policies (NSM Procedure)	159
Chapter 11	Configuring Authentication and Directory Servers	161
	Configuring a Secure Access ACE Server Instance (NSM Procedure)	161
	Creating a Custom Expression for an Authentication Server (NSM Procedure)	163
	Configuring a Secure Access Local Authentication Server Instance (NSM Procedure)	164
	Configuring a Secure Access LDAP Server Instance (NSM Procedure)	167
	Configuring a Secure Access RADIUS Server Instance (NSM Procedure)	171
	Configuring a Secure Access Anonymous Server Instance (NSM Procedure)	174
	Configuring a Secure Access eTrust SiteMinder Server Instance (NSM Procedure)	174
	Configuring a Secure Access Certificate Server Instance (NSM Procedure)	184
	Configuring a Secure Access Manual CA Certificate (NSM Procedure)	185
	Configuring a Secure Access SAML Server Instance (NSM Procedure)	188
	Configuring a Secure Access Active Directory or NT Domain Instance (NSM Procedure)	190
	Configuring a Secure Access NIS Server Instance (NSM Procedure)	193
Chapter 12	Configuring Authentication Realms	195
	Configuring Secure Access Authentication Realms (NSM Procedure)	195
	Configuring Secure Access Authentication Policies (NSM Procedure)	198
	Configuring Secure Access Role Mapping Rules (NSM Procedure)	203
Chapter 13	Configuring Sign-in Policies and Sign-in Pages	207
	Configuring Secure Access Sign-In Policies (NSM Procedure)	207
	Creating Authorization-Only Policies	207
	Creating User or Administrator URLs	209

	Creating Meeting URLs	210
	Configuring Secure Access Sign-In Pages (NSM Procedure)	211
	Creating Users/Administrator Sign-in Pages	211
	Creating Meeting Sign-in Pages	213
Chapter 14	Configuring Single Sign-On	217
	Defining Basic, NTLM, and Kerberos Resources	217
	Configuring Basic, NTLM, and Kerberos Resources (NSM Procedure)	218
	Defining a Basic Authentication, NTLM, or Kerberos Intermediation Resource Policy (NSM Procedure)	221
	Configuring a SAML Access Control Resource Policy (NSM Procedure)	223
	Configuring SAML SSO Artifact Profile Resource Policy (NSM Procedure)	226
Chapter 15	Configuring Secure Access Host Checker Policies	231
	Setting Up Secure Access Device Host Checker Options (NSM Procedure)	231
	Configuring General Host Checker Remediation (NSM Procedure)	233
	Configuring Host Checker Third-Party Applications Using Predefined Rules (NSM Procedure)	234
	Configuring the Remote Integrity Measurement Verifier Server (NSM Procedure)	240
	Configuring Host Checker Customized Requirements Using Custom Rules (NSM Procedure)	241
	Enabling Advanced Endpoint Defense (NSM Procedure)	246
	Enabling Predefined Client-Side Policies for Windows Only (NSM Procedure)	247
	Enabling Connection Control Policies	247
	Configuring Virus Signature Version Monitoring (NSM Procedure)	248
	Importing Virus Signature Version Monitoring or Patch Management Version Monitoring List (NSM Procedure)	249
	Assigning a Proxy Server an Auto-Update Server (NSM Procedure)	249
Chapter 16	Configuring Secure Access Cache Cleaner	251
	Configuring Global Cache Cleaner Options (NSM Procedure)	251
	Configuring Cache Cleaner Restrictions (NSM Procedure)	254
Chapter 17	Configuring Secure Access System Management Features	257
	Configuring the Network Communications Protocol (NSM Procedure)	257
	Configuring Secure Meetings (NSM Procedure)	259
	Configuring Global Security (NSM Procedure)	261
	Configuring Sensors (NSM Procedure)	265
	Creating a Custom Expression for Sensor Settings (NSM Procedure)	268
Chapter 18	Configuring Network Settings	271
	Configuring General Network Settings (NSM Procedure)	271
	Configuring Internal Ports (NSM Procedure)	273
	Configuring Hosts (NSM Procedure)	275
	Configuring Internet Protocol Filters (NSM Procedure)	276
Chapter 19	Synchronizing User Records	277
	Enabling User Record Synchronization (NSM Procedure)	278
	Configuring the Authentication Server (NSM Procedure)	278

	Configuring the User Record Synchronization Server (NSM Procedure)	279
	Configuring the Client (NSM Procedure)	280
	Configuring the Database (NSM Procedure)	281
Chapter 20	Configuring IF-MAP Federation Settings	283
	Configuring IF-MAP Servers (NSM Procedure)	283
	Configuring IF-MAP Client Settings on the Secure Access Device (NSM Procedure)	284
	Configuring IF-MAP Session Export Policy on the Secure Access Device (NSM Procedure)	285
	Configuring IF-MAP Session Import Policy on the Secure Access Device (NSM Procedure)	288
	Configuring IF-MAP Server Replicas (NSM Procedure)	290
Part 4	Managing Secure Access Devices	
Chapter 21	Managing Secure Access Devices	295
	Managing Large Binary Data Files (NSM Procedure)	295
	Removing a Secure Access Device from NSM Management (NSM Procedure)	296
	Archiving Secure Meetings (NSM Procedure)	297
	Managing Secure Access Node from a Cluster	298
Chapter 22	Troubleshooting Secure Access Device Federated Networks	301
	Troubleshooting the IF-MAP Federation Network (NSM Procedure)	301
Part 5	Monitoring Secure Access Devices	
Chapter 23	Configuring Logs in Secure Access Devices	305
	Configuring User Access, Admin Access, Events and Sensors (NSM Procedure)	305
	Configuring Custom Filters and Formats for Log Files (NSM Procedure)	308
	Configuring Client-Side Logs (NSM Procedure)	310
	Configuring Custom Log Filters (NSM Procedure)	311
Chapter 24	Viewing Logs in Secure Access Devices	313
	Viewing Device Status	313
	Viewing Device Monitor Alarm Status	316
	Monitoring the Secure Access as an SNMP Agent (NSM Procedure)	317
Part 6	Index	
	Index	321

About This Guide

- [Objectives on page ix](#)
- [Audience on page ix](#)
- [Document Conventions on page ix](#)
- [List of Technical Publications on page xi](#)
- [Requesting Technical Support on page xii](#)

Objectives

Network and Security Manager (NSM) is a software application that centralizes control and management of your Juniper Networks devices. With NSM, Juniper Networks delivers integrated, policy-based security and network management for all security devices.

Secure Access (SA) device is the next generation Secure Access SSL VPN appliances in its leading market. It enables a solution tailoring to meet the remote and extranet access requirements.

This guide provides the various steps to configure and manage Secure Access using NSM. This guide also helps in understanding of how to configure basic and advanced NSM functionality, including adding new devices, deploying new device configurations, updating device firmware, viewing log information, and monitoring the status of Secure Access.

Audience

This guide is intended for the system administrators who are responsible for configuring Secure Access and Secure Access Federal Information Processing Standards (FIPS).

Document Conventions

[Table 1 on page x](#) defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Table 2 on page x defines text conventions used in this guide.

Table 2: Text Conventions

Convention	Description	Examples
Bold typeface like this	<ul style="list-style-type: none"> Represents commands and keywords in text. Represents keywords Represents UI elements 	<ul style="list-style-type: none"> Issue the clock source command. Specify the keyword exp-msg. Click User Objects
Bold typeface like this	Represents text that the user must type.	user input
<code>fixed-width font</code>	Represents information as displayed on the terminal screen.	<pre>host1# show ip ospf Routing Process OSPF 2 with Router ID 5.5.0.250 Router is an area Border Router (ABR)</pre>
Key names linked with a plus (+) sign	Indicates that you must press two or more keys simultaneously.	Ctrl + d
<i>Italics</i>	<ul style="list-style-type: none"> Emphasizes words Identifies variables 	<ul style="list-style-type: none"> The product supports two levels of access, <i>user</i> and <i>privileged</i>. <i>clusterID</i>, <i>ipAddress</i>.
The angle bracket (>)	Indicates navigation paths through the UI by clicking menu options and links.	Object Manager > User Objects > Local Objects

Table 3 on page xi defines syntax conventions used in this guide.

Table 3: Syntax Conventions

Convention	Description	Examples
Words in plain text	Represent keywords	terminal length
Words in italics	Represent variables	<i>mask</i> , <i>accessListName</i>
Words separated by the pipe () symbol	Represent a choice to select one keyword or variable to the left or right of this symbol. The keyword or variable can be optional or required.	diagnostic line
Words enclosed in brackets ([])	Represent optional keywords or variables.	[internal external]
Words enclosed in brackets followed by and asterisk ([]*)	Represent optional keywords or variables that can be entered more than once.	[level1 level2 11]*
Words enclosed in braces ({ })	Represent required keywords or variables.	{ permit deny } { in out } { clusterId ipAddress }

List of Technical Publications

This section provides the list of the documentations required for any additional information.

Table 4: Network and Security Manager and Secure Access Device Publications

Network and Security Manager Installation Guide	Details the steps to install the NSM management system on a single server or on separate servers. It also includes information on how to install and run the NSM user interface. This guide is intended for IT administrators responsible for the installation and/or upgrade to NSM.
Network and Security Manager Administration Guide	Describes how to use and configure key management features in the NSM. It provides conceptual information, suggested workflows, and examples where applicable. This guide is best used in conjunction with the NSM Online Help, which provides step-by-step instructions for performing management tasks in the NSM UI. This guide is intended for application administrators or those individuals responsible for owning the server and security infrastructure and configuring the product for multi-user systems. It is also intended for device configuration administrators, firewall and VPN administrators, and network security operation center administrators.
Network and Security Manager Configuring Firewall/VPN Devices Guide	Describes NSM features that relate to device configuration and management. It also explains how to configure basic and advanced NSM functionality, including deploying new device configurations, managing Security Policies and VPNs, and general device administration.
Network and Security Manager Online Help	Provides task-oriented procedures describing how to perform basic tasks in the NSM user interface. It also includes a brief overview of the NSM system and a description of the GUI elements.
Secure Access Administration Guide	Provides comprehensive information about configuring the Secure Access appliances.

Table 4: Network and Security Manager and Secure Access Device Publications (*continued*)

Secure Access Quick Start Guide	Provides procedures to install Secure Access appliances on your network and begin configuration.
---------------------------------	--------------------------------------------------------------------------------------------------

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://www.juniper.net/alerts/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.

- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html>.

PART 1

Getting Started

- [Understanding Secure Access Device Configuration on page 3](#)
- [Secure Access Device and NSM Installation Overview on page 7](#)

CHAPTER 1

Understanding Secure Access Device Configuration

- [NSM and Secure Access Device Management Overview on page 3](#)
- [Communication Between a Secure Access Device and NSM Overview on page 3](#)
- [Secure Access Device Services and Device Configurations Supported in NSM on page 5](#)

NSM and Secure Access Device Management Overview

NSM is the Juniper Networks network management tool that allows distributed administration of network appliances. You can use the NSM application to centralize status monitoring, logging, and reporting, and to administer Secure Access device configurations.

With NSM, you can manage most of the parameters that you can configure through the Secure Access admin console. The configuration screens rendered through NSM are similar to the screens in the Secure Access device admin console. NSM incorporates a broad configuration management framework that allows co-management using other methods.

Related Documentation

- [Communication Between a Secure Access Device and NSM Overview on page 3](#)
- [Secure Access Device Services and Device Configurations Supported in NSM on page 5](#)
- [Importing a Secure Access Device on page 11](#)

Communication Between a Secure Access Device and NSM Overview

The Secure Access device and the NSM application communicate through the Device Management Interface (DMI). DMI is a collection of schema-driven protocols that run on a common transport (that is, TCP). DMI is designed to work with Juniper Networks platforms to make device management consistent across all administrative realms. Supported DMI protocols include:

- NetConf (for inventory management, XML-based configuration, text-based configuration, alarm monitoring, and device specific commands).
- Structured syslog.
- Threat flow for network profiling.

DMI supports third-party network management systems that incorporate the DMI standard; however, only one DMI-based agent per device is supported.

The Secure Access device configuration is represented as a hierarchical tree of configuration items. This structure is expressed in XML and can be manipulated with NetConf. NetConf is a network management protocol that uses XML. DMI uses NetConf's generic configuration management capability to allow remote configuration of the device.

To allow NSM to manage the Secure Access device using the DMI protocol, NSM must import the schema and metadata files from the Juniper Networks Schema Repository, a publicly accessible resource that is updated with each device release. In addition to downloading the Secure Access device current schema, NSM may also download upgraded software.

The Schema Repository enables access to XSD and XML files defined for each device, model, and software version.

Before attempting to communicate with NSM, you must first complete the initial configuration of the Secure Access device. Initial configuration includes network interface settings, DNS settings, licensing, and password administration.

If you have several Secure Access devices that will be configured in a clustering environment, the cluster abstraction must first be created in the NSM Cluster Manager. Then you can add individual nodes.

After you have completed the initial network configuration, you can configure the Secure Access device to communicate with NSM using the appropriate network information. Once the Secure Access device has been configured to communicate with NSM, the Secure Access device contacts NSM and establishes a DMI session through an initial TCP handshake.

All communications between the Secure Access device and NSM occur over SSH to ensure data integrity.

After the Secure Access device initially contacts NSM and a TCP session is established, interaction between the Secure Access device and NSM is driven from NSM, which issues commands to get hardware, software, and license details of the Secure Access device. NSM connects to the Schema Repository to download the configuration schema that is specific to the Secure Access device.

NSM then issues a command to retrieve configuration information from the Secure Access device. If NSM is contacted by more than one Secure Access device as a member of a cluster, information from only one of the cluster devices is gathered. NSM attempts to validate the configuration received from the Secure Access device against the schema from Juniper Networks.

Once the Secure Access device and NSM are communicating, the Secure Access device delivers syslog and event information to NSM.

After NSM and the Secure Access device are connected, you can make any configuration changes directly on the Secure Access device, bypassing NSM. NSM automatically detects these changes and imports the new configuration data. Changes to Secure Access cluster members will similarly be detected by NSM.

When you make changes to the Secure Access device configuration through NSM you must push the changes to the device by performing an Update Device operation.

When you double-click the Secure Access device icon in the Device Manager and select the Configuration tab, the configuration tree appears in the main display area in the same orientation as items appear on the Secure Access device admin console.

- Related Documentation**
- [Secure Access Device Services and Device Configurations Supported in NSM on page 5](#)
 - [Importing a Secure Access Device on page 11](#)
 - [NSM and Secure Access Device Management Overview on page 3](#)

Secure Access Device Services and Device Configurations Supported in NSM

The Secure Access device supports the following services in NSM:

- Inventory management service — Enables management of the Secure Access software, hardware, and licensing details. Adding or deleting licenses or upgrading or downgrading software are not supported.
- Status monitoring service — Allows the Secure Access device's status to be obtained, including name, domain, OS version, synchronization status, connection details, and current alarms.
- Logging service — Allows the Secure Access device's logs to be obtained in a time-generated order. Logging configuration details that are set on the Secure Access device will apply to NSM.
- XML-based configuration management service — Enables NSM to manage the configuration of the Secure Access device. NSM uses the same XML schema as the Secure Access device, so you can troubleshoot NSM using XML files downloaded from the Secure Access device.

The following device configurations are not supported:

- Editing licensing information, although licenses can be viewed
- Creating clusters, joining nodes to clusters, or enabling or disabling cluster nodes
- Packaging log files or debug files for remote analysis
- Rebooting the Secure Access device

- Related Documentation**
- [Communication Between a Secure Access Device and NSM Overview on page 3](#)

- [NSM and Secure Access Device Management Overview on page 3](#)

CHAPTER 2

Secure Access Device and NSM Installation Overview

- [Secure Access Device Installation Overview on page 7](#)
- [NSM Installation Overview on page 7](#)

Secure Access Device Installation Overview

Before beginning, see the *Juniper Networks Security Products Safety Guide* for important safety information.

You can install the Secure Access device and start configuring your system using the following steps:

1. Rack mount the Secure Access device.
2. Install the hardware.
3. Perform basic setup.
4. License and configure your Secure Access device.

See the *Quick Start Guide for Secure Access 2500, 4500 and 6500* to install and configure a Secure Access device.

Related Documentation

- [NSM Installation Overview on page 7](#)
- [Communication Between a Secure Access Device and NSM Overview on page 3](#)

NSM Installation Overview

NSM is a software application that enables you to integrate and centralize management of your Juniper Networks environment. You need to install two main software components to run NSM: the NSM management system and the NSM user interface (UI).

See the *Network Security Manager Installation Guide* for the steps to install the NSM management system on a single server or on separate servers. It also includes information on how to install and run the NSM user interface. The *Network Security Manager Installation Guide* is intended for IT administrators responsible for installing or upgrading to the NSM.

- Related Documentation**
- [Communication Between a Secure Access Device and NSM Overview on page 3](#)
 - [Secure Access Device Installation Overview on page 7](#)

PART 2

Integrating Secure Access Devices

- [Adding Secure Access Devices on page 11](#)
- [Adding Secure Access Clusters on page 23](#)
- [Working with Secure Access Templates on page 29](#)

CHAPTER 3

Adding Secure Access Devices

This chapter provides information on how to add a Secure Access device through the import workflow and also how to verify the imported configuration. This chapter contains the following procedures:

- [Importing a Secure Access Device on page 11](#)
- [Requirements for Importing a Secure Access Device into NSM Through a Reachable Workflow on page 14](#)
- [Adding a Secure Access Device Through a Reachable Workflow on page 15](#)
- [Importing Multiple Secure Access Devices on page 16](#)
- [Verifying Imported Device Configurations on page 19](#)

Importing a Secure Access Device

You can add a Secure Access device to your existing network by using NSM and importing its configurations. Using the Add Device Wizard, you can configure a connection between the management system and the physical device, and then import all device parameters, policies, objects, VPNs, and so on.

Import a Secure Access device by following these procedures:

1. [Installing and Configuring a Secure Access Device on page 11](#)
2. [Adding a Secure Access Device Through NSM on page 12](#)
3. [Configuring and Activating the NSM agent on the Secure Access Device on page 13](#)
4. [Confirming Connectivity and Importing the Secure Access Device Configuration on page 14](#)

Installing and Configuring a Secure Access Device

Before you add the Secure Access device to NSM, you must install and configure the Secure Access device to have logon credentials for an NSM administrator.

To install and configure a Secure Access device:

1. Select **System > Network > Overview** in the device's admin console and ensure that basic connection information such as the following are configured on the Secure Access device:
 - Network interface settings
 - DNS settings
 - Password
2. Select **Authentication > Auth Servers** and enter the username and password of the NSM administrator in the applicable authentication server.



NOTE: Only password-based authentication servers can be used. One-time password authentication is not supported.

3. Select **Administrators > Admin Roles** and create an NSM agent role.
4. Select **Administrators > Admin Realms** and create an NSM agent administrator realm for the DMI agent on the Secure Access device and use role mapping to associate the NSM agent role and realm. Do not apply any role or realm restrictions for the NSM agent role or realm.

For complete details on installing and configuring Secure Access devices, see the *Juniper Networks Secure Access Administration Guide*.

Adding a Secure Access Device Through NSM

To add the Secure Access device through the NSM UI:

1. From the left pane of the NSM UI, click **Configure**.
2. Expand **Device Manager** and Select **Devices**. The Devices workspace appears on the right side of the screen.
3. Click the **Device Tree** tab, click the **New** button, and select **Device**. The New-Device dialog box appears.
4. Select **Device is Not Reachable** and click **Next**.
5. Enter the device name, and select the required color, OS name (SA), and platform and managed OS version from the drop-down lists.
6. From the Choose Device Server Connection Parameter area, select:
 - **Use Default Device Server IP Address and Port** — Connects the device to the NSM Device Server IP address and port.
 - **Use Device Server Through MIP** — Connects the NSM device server through a mapped IP address and port.
7. Click **Next**, and a unique external ID gets generated automatically. This ID represents the device within the management system.

8. Enter an admin username for the device admin.
9. Set the Admin User Password and the First Connection One-Time Password:
 - Select **Set Password** and enter a new password.
 - Confirm your new password and click **OK**.

**NOTE:**

- Make a note of the unique external ID. The device administrator will need it to configure connectivity with NSM. The wizard automatically enters this value for the device. This ID number represents the device within the management system.
- Specify the administrator username and password for the SSH connection. This name and password must match the name and password already configured on the device.
- Specify the First Connection One Time Password (OTP) that authenticates the device. Make a note of this password. The device administrator will need it to configure the connectivity with NSM.

10. Click **Finish** to add the device to the NSM UI. The newly added Secure Access device appears in the Devices workspace.

Configuring and Activating the NSM agent on the Secure Access Device

You must configure and activate the NSM agent on the Secure Access device. It establishes the SSH communications with the NSM application and controls the Secure Access device from the NSM application.

To configure and activate the NSM agent:

1. Select **System > Configuration > DMI Agent** to add the NSM management application.
2. Under DMI settings for outbound connections, enter the device server's IP address in the Primary Server box.
3. Enter **7804** in the Primary Port box.
4. Fill in the Backup Server and Backup Port boxes, if a device server is configured for high availability.
5. Enter the unique external ID provided by the NSM administrator in the Device ID box.
6. Enter the first connection one-time password provided by the NSM administrator in the HMAC box.
7. Click **Enable** to activate the NSM agent.
8. Click **Save Changes**, and the device attempts to establish a session with the NSM application.

The device software initiates the TCP connection to NSM and identifies itself using the specified device ID and HMAC. Both sides then engage in SSH Transport Layer interactions

to set up an encrypted tunnel. The Inbound and Outbound DMI connections enabled facilitates the DMI connection. The DMI uses the specified admin realm to login to the device. The NSM application authenticates itself to the Secure Access device based on username and password.

Confirming Connectivity and Importing the Secure Access Device Configuration

To confirm connectivity:

1. From the Devices workspace, select the **Device List** tab.
2. Check the newly added device in the Connection Status column. The connection status must change from Never Connected to Up.

If the connection status appears as Device Platform Mismatch or Device Firmware Mismatch, delete the device from the application and add it back using the correct device platform and managed OS, respectively.

To import the device configuration:

1. From the Devices workspace, select the **Device List** tab.
2. Right-click the newly added Secure Access device and select **Import Device**. The Save Changes dialog box appears.
3. Click **Yes** to save policy or VPN changes. The Device Import Option dialog box appears.
4. Select **Run Summarize Delta Config**, click **OK** and **Yes**. The Job Information dialog box displays the progress of the delta config summary. You can also monitor the progress in the Job Manager.

The next step is to verify the imported configuration using either the Device Monitor or the Device Manager in NSM. See “Verifying Imported Device Configurations” for details.

Related Documentation

- [Importing Multiple Secure Access Devices on page 16](#)
- [Verifying Imported Device Configurations on page 19](#)
- [Creating and Applying a Secure Access Device Template on page 29](#)

Requirements for Importing a Secure Access Device into NSM Through a Reachable Workflow

Adhere to the following requirements to import a Secure Access device into NSM through a reachable workflow:

- The inbound DMI connection must be enabled in the Secure Access device.
- SSH port must be configured in the Secure Access device. The default SSH port is 22.
- The DMI agent admin realms must be configured and an admin user must be mapped to a role with full admin privileges.

- Related Documentation**
- [Adding a Secure Access Device Through a Reachable Workflow on page 15](#)
 - [Verifying Imported Device Configurations on page 19](#)

Adding a Secure Access Device Through a Reachable Workflow

To import a Secure Access device through a reachable workflow into NSM:

1. From the left pane of the NSM UI, click **Configure**.
2. Expand **Device Manager** and select **Devices**. The Devices workspace appears on the right side of the screen.
3. Click the **Device Tree** tab, click the **New** button, and select **Device**. The New Device dialog box appears.
4. Select **Device is Reachable** and click **Next**.
5. Enter the following connection information:
 - Enter the IP address of the device.
 - Enter the username of the device administrator.
 - Enter the password for the device administrator.
 - Select SSH V2 as the connection method.
 - Ensure that the TCP port number is 22.
6. Click **Next**. The Verify Device Authenticity dialog box opens. The Add Device wizard displays the RSA Key FingerPrint information. To prevent man-in-the-middle attacks, you should verify the fingerprint using an out-of-band method.
7. Click **Next** to accept the fingerprint. The Detecting Device dialog box opens.
8. After the wizard displays the autodetected device information, verify that the device type, OS version, and the device serial number are correct. The wizard also detects the hostname configured on the device. You can either use the hostname as the NSM device name or you can enter a new name in the text box provided.
9. Click **Next** after verifying the auto detected device information.
10. Click **Finish** to add the device to the NSM UI. The Secure Access device appears in the Devices workspace.

- Related Documentation**
- [Requirements for Importing a Secure Access Device into NSM Through a Reachable Workflow on page 14](#)
 - [Importing a Secure Access Device on page 11](#)

Importing Multiple Secure Access Devices

If your network includes a large number of devices, you can save time by adding multiple devices in a single workflow. You can add up to 4000 devices at a time to a single domain (but you cannot add multiple devices to different domains at one time).

Add multiple Secure Access devices by following these procedures:

1. [Creating the CSV File on page 16](#)
2. [Validating the CSV File on page 17](#)
3. [Adding and Importing Multiple Secure Access Devices on page 18](#)

Creating the CSV File

The CSV file defines all the required and optional values for each Secure Access device. Within a .csv file, you define the Secure Access device configuration values that you want to add. The required and optional values depend not only on how the Secure Access devices are deployed on your network but also on the device family.

Juniper Networks provides CSV templates in Microsoft Excel format for each type of CSV file. These templates are located in the utils subdirectory where you have stored the program files for the UI client. For example:

C:\Program Files\Network and Security Manager\utils

For each CSV file, each row defines a single Secure Access device's values for each parameter. For text files, columns are separated by commas.

Creating Secure Access Device Parameters in CSV File

For a Secure Access device, [Table 5 on page 16](#) lists the parameters to be set in the CSV file:

Table 5: CSV File Information for Secure Access Devices

Field	Type	Required	Acceptable Values
Name	String	yes	sa-6500(FIPS), sa-6500, sa-6000(FIPS), sa-6000, sa-4500(FIPS), sa-4500, sa-4000(FIPS), sa-4000, sa-2500, sa-2000
Color	String	yes	blue, red, green, yellow, cyan, magenta, orange, pink
OS Name	String	yes	SA
Platform	String	yes	SA-2000, SA-2500, SA-4000, SA-4000(FIPS), SA-4500, SA-4500(FIPS), SA-6000, SA-6000(FIPS), SA-6500, SA-6500(FIPS)

Table 5: CSV File Information for Secure Access Devices (*continued*)

Device Subtype	String	yes	Set to "none"
Managed OS Version	String	yes	6.3
Device Admin Name	String	yes	
Device Admin Password	String	yes	Must be a minimum of nine characters

Using an Excel File to Add Multiple Secure Access Devices

To edit the Excel file to add multiple Secure Access devices:

1. Copy and open either the **bulkadd_nonreachable-sample.csv** file or the **bulkadd_nonreachable-DMI-sample.csv** file located in **C:/Program Files/Network and Security Manager/utis**.
2. Using one row for each Secure Access device you want to add, enter the required values for each parameter that you wish to set for them. You can also provide optional values, if desired.
3. Save the file to a location on your local drive.

Using a Text File to Add Multiple Secure Access Devices

To add multiple Secure Access devices, create a text file with the following text:

1. Open a Text file and add the Secure Access devices and its parameters as follows.

SA-4000, blue, SA, SA-4000, none, root, 6.3, netscreen
SA-4500, pink, SA, SA-4500, none, root, 6.3, netscreen
SA-6000, cyan, SA, SA-6000, none, root, 6.3, netscreen
SA-6500, pink, SA, SA-6500, none, root, 6.3, netscreen
2. Save the file as a .csv file.

Validating the CSV File

When you add the Secure Access devices, NSM validates the configuration information in the .csv file and creates a validation report. The report lists any incorrect or duplicate configurations, and indicates the exact line that contains invalid data.



NOTE: The validation report displays only the first error in the line. If the line contains additional errors, those errors do not appear in the validation report.

Select **Cancel** to quit adding multiple Secure Access devices, or select **Add Valid Devices** to begin adding the Secure Access devices for which you have provided valid device configurations.

If the validation report listed incorrect configurations, you can still select **Add Valid Devices**; however, only the devices with correct configurations are added. If the .csv file contains duplicate configurations, NSM ignores the duplicates.

After you have added multiple Secure Access devices, you cannot roll back or undo your changes. To edit or delete Secure Access devices, select the Secure Access device in the UI and make the necessary changes.

Adding and Importing Multiple Secure Access Devices

To add and import multiple Secure Access devices in the NSM UI:

1. From the left pane of the NSM UI, click **Configure**.
2. Expand **Device Manager** and select **Devices**. The Devices workspace appears on the right side of the screen.
3. Click the **Device Tree** tab, click the **New** button, and select **Many Devices**. The New - Device dialog box appears
4. In the New-Device dialog box:
 - Select **Device is Not Reachable**.
 - Specify the location of the CSV file.
 - Specify the output directory for the .cli file. For each valid device configuration that uses a dynamic IP address, NSM creates a .cli output file. By default, the .cli file is saved to the following GUI server directory:

```
/usr/netscreen/GuiSvr/var/ManyDevicesOutput/<inputFile_YYYYMMDDHHMM>/
```
5. Click **Next**. The Add Device wizard validates the CSV file and provides a validation report.
 - Select **Cancel** to quit the Add Many Devices process.
 - Select **Add Valid Devices** to begin adding the devices for which you have provided valid device configurations.
6. From the **Choose Device Server Connections Parameter** area, enter information as required. Use the default settings to configure the device to connect to the NSM device server IP address and port. Use an MIP to configure the device to connect to the NSM device server through a mapped IP address and port.
7. Click **Finish** to add the Secure Access devices.

The time it takes for NSM to activate and import the Secure Access devices depends on the number of Secure Access devices and the management system configuration.

Related Documentation

- [Verifying Imported Device Configurations on page 19](#)
- [Adding a Secure Access Cluster Overview on page 23](#)
- [Adding a Secure Access Cluster with Imported Cluster Members on page 24](#)

- [Importing a Secure Access Device on page 11](#)
- [Creating and Applying a Secure Access Device Template on page 29](#)

Verifying Imported Device Configurations

After importing a Secure Access device, you should verify whether all device information has been imported.

The imported device configurations can be verified in any of the following ways:

- [Using Device Monitor on page 19](#)
- [Using Device Manager on page 19](#)
- [Using Job Manager on page 20](#)
- [Using Configuration Summaries on page 20](#)

Using Device Monitor

The Device Monitor in NSM tracks the status of individual devices, systems, and their processes. To check the status of the imported device in the Device Monitor, from the left pane click **Investigate**, expand **Realtime Monitor**, and select **Device Monitor**. From the Device Monitor workspace, check the following parameters for your imported device:

- The Config Status must be Managed.
- The Conn. Status must be Up.

Using Device Manager

Using the Device Manager in NSM you can verify the configuration settings of the imported device. To verify the configuration settings, click **Configure**, expand **Device Manager**, and select **Devices List** tab.

Ensure that the following parameters are indicated:

- Imported device serial number matches the serial number on the physical device.
- Imported device IP address matches the IP address for the physical device.
- Imported device administrator name and password are correct for the physical device.



NOTE: All passwords handled by NSM are case-sensitive.

- Imported device interfaces are correct for the physical device.
- Management system successfully imported all device configuration information, including zones, virtual routers, and routes.

Using Job Manager

Job Manager tracks the status of major administrative tasks, such as importing or updating a device. After you import a device, view the report for the import task to ensure that the management system imported the device configuration as you expected. To track the status of the imported Secure Access devices in NSM, from the left pane, click **Administer** and select **Job Manager**.



NOTE: Job Manager configuration summaries and job information details do not display passwords in the list of CLI commands for administrators who do not have the assigned activity "View Device Passwords." By default, only the super administrator has this assigned activity.

Job Manager also tracks the status of configuration summaries, described in the **Using Configuration Summaries** section.

Using Configuration Summaries

NSM provides three configuration summaries to help you manage device configurations and prevent accidental misconfigurations. Use configuration summaries after you import a device to ensure that the management system imported the physical device configuration as you expected.

Configuration summaries help with ongoing device maintenance, particularly for devices on which a local device administrator has been troubleshooting using CLI commands or the Web UI. Because the device object configuration in the NSM UI can overwrite the physical device configuration, you should always confirm the commands that are sent to the device.

The three configuration summaries that help you to manage device configurations are:

- Configuration Summary
- Delta Configuration Summary
- Running Configuration Summary

Configuration Summary

A configuration summary shows you the exact CLI commands that will be sent to the managed device during the next device update. To get a configuration summary in NSM, from the Devices menu, click **Configuration** and select **Summarize Config**. The Summarize Config dialog box appears. You see a list of security devices to which you have access. Select the device you just imported and click **OK**. NSM analyzes the UI device object configuration and generates a summary report that lists the CLI commands or XML messages to send to the physical device during the next device update.

For a just-imported device, the configuration summary report displays the device configuration that matches the configuration currently running on the physical device.

Delta Configuration Summary

A delta configuration summary shows you the differences between the configuration you see in the NSM UI and the configuration on the physical device. To get a delta configuration summary in NSM, from the Devices menu click **Configuration** and select **Summarize Delta Config**. The Get Delta Config Summary dialog box appears with a list of devices to which you have access. Select the device you just imported and click **OK**. NSM queries the physical device to obtain a list of all CLI commands or XML messages used in the device configuration, compares that list with the UI device configuration, and generates a summary report of all differences, or deltas, discovered.

For a just-imported device, the delta config summary displays minimal deltas, meaning that very few differences exist between the configuration on the physical device and the configuration in the UI. NSM automatically imports your VPNs and displays the VPN policies; however, NSM does not create VPN abstractions for your VPN policies.

Get Running Configuration

A running configuration summary shows you the exact CLI commands or XML messages that were used to create the current device configuration on the physical device. To get the running config summary in the NSM application, from the Devices menu click **Configuration** and select **Get Running Config**. The Get Running Config dialog box appears. You see a list of devices to which you have access. Select the device you just imported and click **OK**.

NSM queries the physical device to obtain a list of all CLI commands used in the device configuration and generates a summary report that lists those commands. For a just-imported device, the get running config summary report displays the device configuration currently running on the physical device.

Related Documentation

- [Adding a Secure Access Cluster Overview on page 23](#)
- [Adding a Secure Access Cluster with Imported Cluster Members on page 24](#)
- [Creating and Applying a Secure Access Device Template on page 29](#)
- [Importing Multiple Secure Access Devices on page 16](#)

Adding Secure Access Clusters

- [Adding a Secure Access Cluster Overview on page 23](#)
- [Adding a Secure Access Cluster with Imported Cluster Members on page 24](#)

Adding a Secure Access Cluster Overview

When you add a Secure Access cluster in NSM, you first add the cluster and then add each member. Adding a member is similar to adding a standalone device.

Secure Access clusters can be configured by the device administrator to operate in active/passive mode or in active/active mode. Clusters in active/passive mode are made up of a primary member and a secondary member. All traffic flows through the primary member. If the primary member fails, then the secondary member takes over.

In active/active mode, traffic is load-balanced across all cluster members. If one member fails, then load balancing takes place among the surviving members.

In active/active Network Connect (NC) deployments, we recommend that you do the following:

- Split the NC IP pool into node-specific subpools.
- Perform static route configuration on the backend router infrastructure in a coordinated fashion, with static routes to each subpool pointing to the internal IP address of the hosting cluster node as the next-hop gateway.



NOTE: The Secure Access device does not support a common IP address pool for NC for an active/active cluster.

The number of members permitted in a cluster depends on whether the cluster is configured in active/active mode or in active/passive mode. You can have no more than two cluster members in active/passive mode. In active/active mode you can have up to eight members.

Before you can activate a cluster member in NSM, the device administrator must have already created the cluster and added, configured, and enabled the physical cluster member. See the *Juniper Network Secure Access Administration Guide* for details on creating and configuring clusters.

Secure Access devices configured in a cluster must have a cluster object and member objects defined in the NSM before the Secure Access cluster nodes can be recognized by NSM. Nodes from this cluster that subsequently contact NSM will be represented by fully functional member icons in the Cluster Manager. Cluster members whose DMI agents do not contact NSM will be displayed in the NSM Device Monitor as unconnected devices.

Secure Access devices use member IDs to identify each cluster member object. When importing cluster members, the member ID is imported as part of the cluster.

To add a Secure Access cluster to NSM, first add the cluster object, and then add its members. You add cluster members one at a time, in a similar manner to adding standalone devices.



NOTE: Adding a cluster and adding a cluster member have no effect on the cluster itself. The cluster and cluster members must already exist.

Once a Secure Access cluster is managed by NSM, subsequent changes applied to the cluster by NSM will be synchronized by the cluster across all cluster members. Similarly, changes to a Secure Access cluster membership that occur through administrator action on the native device UI will be reflected back to NSM, and NSM will display the modified cluster.

You can add a Secure Access cluster from your existing network into NSM and import their configurations. Using the Add Device Wizard, you configure a connection between the management system and the physical device, and then import all device parameters.

**Related
Documentation**

- [Adding a Secure Access Cluster with Imported Cluster Members on page 24](#)
- [Creating and Applying a Secure Access Device Template on page 29](#)
- [Promoting a Secure Access Device Configuration to a Template on page 31](#)

Adding a Secure Access Cluster with Imported Cluster Members

Add and import a Secure Access cluster in NSM by following these procedures:

1. [Installing and Configuring the Cluster on page 25](#)
2. [Adding the Cluster in NSM on page 25](#)
3. [Adding the Cluster Members in NSM on page 25](#)
4. [Configuring and Activating the DMI Agent on the Cluster on page 27](#)
5. [Importing Cluster Configuration on page 27](#)

Installing and Configuring the Cluster

You must install and configure the Cluster to have logon credentials for an NSM administrator before you can add the cluster to NSM.

Adding the Cluster in NSM

Before you can add a Secure Access device cluster to NSM, you must first add the cluster object, and then add its members.

To add new cluster to NSM:

1. From the left pane of the NSM UI, click **Configure**.
2. Expand **Device Manager** and select **Devices**. The Devices workspace appears on the right side of the screen.
3. Click the **Device Tree** tab, click the **New** button, and select **Cluster**. The New - Cluster dialog box appears.
4. Enter the cluster name and select the required color, OS name (SA), and platform and managed OS version from the drop-down lists.
5. Click **OK**, The new cluster appears in the Device Manager.

Adding the Cluster Members in NSM

You add cluster members one at a time, in a similar manner to adding standalone devices.

Adding Cluster Members through Not Reachable Workflow

To add a cluster member through the non-reachable workflow:

1. From the left pane of the NSM UI, click **Configure**.
2. Expand **Device Manager** and select **Devices**. The Devices workspace appears on the right side of the screen.
3. Click the **Device Tree** tab, and select the cluster to which you want to add the members.
4. Click the **New** button and select **Cluster Member**. The New-Cluster Member dialog box appears.
5. Enter the cluster member name, select **Device Is Not Reachable**, and click **Next**.
6. From the Choose Device Server Connections Parameter area, select:
 - **Use Default Device Server IP Address and Port**—Connects the device to the NSM device server IP address and port.
 - **Use Device Server Through MIP**—Connects to the NSM device server through a mapped IP address and port.
7. Click **Next**, and a unique external ID gets generated automatically. This ID represents the device within the management system.
8. Enter an admin username for the device admin.

9. Set the admin user password and the first connection one-time password:
 - a. Enter a new password in the **Set Password** box.
 - b. Confirm the new password and click **OK**.



NOTE:

- Make a note of the unique external ID. The device administrator will need it to configure connectivity with NSM. The wizard automatically enters this value for the device. This ID number represents the device within the management system.
 - Specify the administrator username and password for the SSH connection. This name and password must match the name and password already configured on the device.
 - Specify the first connection one time password (OTP) that authenticates the device. Make a note of this password. The device administrator will need it to configure the connectivity with NSM.
-

10. Click **Finish** to add the cluster member to the NSM GUI. The cluster member appears in the Devices workspace.

Adding Cluster Members through Reachable Workflow

To add a cluster member:

1. From the left pane of the NSM UI, click **Configure**.
2. Expand **Device Manager** and select **Devices**. The Devices workspace appears on the right side of the screen.
3. Click the **Device Tree** tab, and select the cluster to which you want to add the members.
4. Click the **New** button and select **Cluster Member**. The New–Cluster Member dialog box appears.
5. Enter the cluster member name, select **Device Is Reachable** and click **Next**.
6. Specify the device connection settings:
 - **IP Address**—IP address of the Secure Access device.
 - **Admin User Name**—Administrator user name created for the Secure Access device.
 - **Password**—Administrator password created for the Secure Access device.
7. Click **Next**, The Secure Access device is detected and the device details are displayed.
8. Enter a new name for the Secure Access device in **Device Name** to change the host name of the device.
9. Click **Finish** to add the cluster member to the NSM GUI. The cluster member as a child of the Secure Access cluster in the Devices workspace.

Configuring and Activating the DMI Agent on the Cluster

On each cluster member device, configure and activate the DMI agent and establish an SSH session with NSM.

Importing Cluster Configuration

After adding the cluster members, you must import the cluster configurations. You do this only once and for the entire cluster because the configuration is identical for all cluster members.

To import the cluster configuration:

1. From the left pane of the NSM UI, click **Configure**.
2. Expand **Device Manager** and select **Devices**. The Devices workspace appears on the right side of the screen.
3. Click the **Device Tree** tab. Right-click the cluster to which you want to import the configurations, and select **Import Device**.

NSM starts to import the configuration and a job window reports the progress of the job. When the job finishes, the configuration status for each cluster member in the Device List tab changes from Import Needed to Managed.

After importing, the configuration appears at the cluster level in NSM. To edit the configuration, open the cluster icon, not the individual cluster members.

Related Documentation

- [Creating and Applying a Secure Access Device Template on page 29](#)
- [Promoting a Secure Access Device Configuration to a Template on page 31](#)
- [Adding a Secure Access Cluster Overview on page 23](#)

CHAPTER 5

Working with Secure Access Templates

- [Creating and Applying a Secure Access Device Template on page 29](#)
- [Promoting a Secure Access Device Configuration to a Template on page 31](#)

Creating and Applying a Secure Access Device Template

You can create and apply configuration templates for setting up new Secure access devices through NSM.

Create and apply templates by following these procedures:

1. [Creating the Template on page 29](#)
2. [Applying the Template on page 30](#)

Creating the Template

To create a Secure Access template:

1. From the left pane of the NSM UI, click **Configure**.
2. Expand **Device Manager** and select **Device Templates**. The Device Templates workspace appears on the right side of the screen.
3. Click the **Device Template Tree** tab, click the **New** button, and select **SA Template**. The New Device Template dialog box appears.
4. Name the Secure Access device template, and select a color for the template.
5. Enter the following basic information:
 - Device description
 - IP address
 - Admin username
 - Admin user password
6. Click **OK** to save the template. The newly created templates will appear under the Device Template Tree.
7. Double-click the newly created template to enter the configuration information. The Device Template screen appears.

8. Click the **Configuration** tab; select the required parameters on the left pane and specify the appropriate values.
9. Click **OK** to create a Secure Access device template.

You can now use this template when configuring Secure Access devices.



NOTE: You can create a custom expression in a device template, but you cannot validate the custom expression. The Validate button is not enabled in the Custom Expressions editor for device templates.

Applying the Template

To apply a template to a Secure Access device:

1. From the left pane of the NSM UI, click **Configure**.
2. Expand **Device Manager** and select **Devices**. The Devices workspace appears on the right side of the screen.
3. Double-click the Secure Access device to open the device editor.
4. From the Device Info tab, select **Templates**. The templates configuration screen appears.
5. Click the **Edit** icon. The Edit Templates dialog box appears.
6. Select the required template from the list, and click **OK** in the Edit Templates dialog box.
7. In the templates configuration screen, select **Retain template values on removal** to retain template values if a template is removed from the device.
8. Select the required template from the list and apply the required settings as explained in [Table 6 on page 30](#) and click **OK**.

Table 6: Template Operations Settings

Option	Function
Add templates with lowest priority	Adds the templates with the least priority.
Add templates with highest priority	Adds the templates with the highest priority.
Remove templates	Removes the templates.
Don't change templates	Does not accept modifications to the templates.
Remove conflicting device values	Does not add device values that conflict.
Report irrelevant template values	Reports irrelevant template values.
Report conflicts with other templates	Reports conflicts with other templates.

Table 6: Template Operations Settings (*continued*)

Validate	Validates the templates.
-----------------	--------------------------

To apply the settings to the device itself, run the Update Device directive to push the configuration to the device.

**Related
Documentation**

- [Promoting a Secure Access Device Configuration to a Template on page 31](#)
- [Configuring Secure Access Device User Roles \(NSM Procedure\) on page 35](#)
- [Verifying Imported Device Configurations on page 19](#)

Promoting a Secure Access Device Configuration to a Template

NSM allows you to import a Secure Access device configuration and then convert, or promote, it to a template. You can then use that template to make identical configurations on other Secure Access devices.

To promote a Secure Access device configuration to a template:

1. From the Devices workspace in NSM, double-click the Secure Access device whose configuration settings you want to promote to a template. The Secure Access device dialog box appears.
2. Select the Configuration node. The device editor appears.
3. From the left pane of the device editor, right-click the Configuration node that you want to promote to a template and select **Promote Template**. The Select templates dialog box appears.
4. Select the template to which you want to apply the configuration settings and click **OK**. The Secure Access device configuration is promoted to the selected template.

**Related
Documentation**

- [Verifying Imported Device Configurations on page 19](#)
- [Creating and Applying a Secure Access Device Template on page 29](#)

PART 3

Configuring Secure Access Devices

- [Configuring User Roles and Administrator Roles on page 35](#)
- [Configuring Terminal Services Using Remote Access Mechanism on page 51](#)
- [Configuring Access Options using Remote Access Mechanisms on page 65](#)
- [Configuring Secure Access Resource Profiles on page 93](#)
- [Configuring Secure Access Resource Policies on page 137](#)
- [Configuring Authentication and Directory Servers on page 161](#)
- [Configuring Authentication Realms on page 195](#)
- [Configuring Sign-in Policies and Sign-in Pages on page 207](#)
- [Configuring Single Sign-On on page 217](#)
- [Configuring Secure Access Host Checker Policies on page 231](#)
- [Configuring Secure Access Cache Cleaner on page 251](#)
- [Configuring Secure Access System Management Features on page 257](#)
- [Configuring Network Settings on page 271](#)
- [Synchronizing User Records on page 277](#)
- [Configuring IF-MAP Federation Settings on page 283](#)

CHAPTER 6

Configuring User Roles and Administrator Roles

- [Configuring Secure Access Device User Roles \(NSM Procedure\) on page 35](#)
- [Creating Secure Access Role-Based Source IP Alias \(NSM Procedure\) on page 38](#)
- [Configuring Secure Access General Session Options \(NSM Procedure\) on page 39](#)
- [Creating and Configuring Secure Access Device Administrator Roles \(NSM Procedure\) on page 43](#)

Configuring Secure Access Device User Roles (NSM Procedure)

A user role is an entity that defines user session parameters, personalization settings, and enabled access features. You can customize a user role by enabling specific Secure Access device access features, defining Web, application, and session bookmarks, and configuring session settings for the enabled access features. You can create and configure user roles through the User Roles page from the Secure Access device configuration tree.

To configure a user role:

1. In the NSM navigation tree, select **Device Manager** > **Devices**. Click the **Device Tree** tab and then, double-click the Secure Access device for which you want to configure user roles.
2. Click the **Configuration** tab, select **Users** > **User Roles**. The corresponding workspace appears.
3. Click the **New** button and the New dialog box appears.
4. Add or modify settings on the General tab page as specified in [Table 7 on page 36](#).
5. Add or modify global role options on the Global Role Options tab page as specified in [Table 8 on page 37](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 7: User Role Configuration Details

Option	Function	Your Action
General tab		
Name	Specifies a unique name for the user role.	Enter a name.
General > Overview tab		
Description	Describes the user role.	Enter a brief description for the user role.
VLAN/Source IP	Specifies role-based source IP aliases.	Select General > VLAN/Source IP to apply settings for the role.
Session Options	Specifies the session time limits, roaming capabilities, session and password persistency, request follow-through options, and idle timeout application activity.	Select General > Session Options to apply settings for the role.
UI Options	Specifies customized settings for the Secure Access device welcome page and the browsing toolbar for users mapped to this role.	Select General > UI Options to apply custom settings for the role; otherwise, the Secure Access device uses the default settings.
Web	Enables you to intermediate Web URLs through the Content Intermediation Engine.	Select General > Web to enable this access feature for the role.
Windows Files	Controls access to resources on Windows server shares.	Select General > Windows Files to enable this access feature.
NFS Files	Controls access to resources on UNIX/NFS servers.	Select General > NFS Files to enable this access feature.
Secure Application Manager	Provides secure, application-level remote access to enterprise servers from client applications.	Select General > Secure Application Manager to enable this access feature.
Telnet/SSH	Enables users to connect to internal server hosts in the clear using Telnet protocols or to communicate over an encrypted Secure Shell (SSH) session through a Web-based terminal session emulation.	Select General > Telnet/SSH to enable this access feature.

Table 7: User Role Configuration Details (*continued*)

Option	Function	Your Action
Terminal Services	Enables terminal emulation sessions on a Windows terminal server, Citrix NFuse server, or Citrix Metaframe server.	Select General > Terminal Services to enable this access feature.
Meeting	Allows users to securely schedule and hold online meetings between both Secure Access devices and non-Secure Access devices.	Select General > Meeting to enable this access feature.
Email	Enables users to use standards-based e-mail clients to access corporate e-mail securely from remote locations without the need for any additional software, such as a VPN client.	Select General > Email to enable this access feature.
Network Connect	The Network Connect option provides secure, SSL-based network-level remote access to all enterprise application resources using the Secure Access device over port 443.	Select General > Network Connect to enable this access feature.

Table 8: Global User Role Configuration Details

Option	Function	Your Action
Global Role Options > Global Terminal Services Role Options tab		
Citrix Client CAB File	Allows you to specify a shared binary data object.	Select the plus button to specify the name, color, comment and file name for the object.
Name	Specifies the name of the object. NOTE: The name, color, comment, file name fields are displayed only when you click the plus button in the right side of the Citrix Client CAB File list.	Enter the name.
Color	Specifies the color of the object.	Select a color from Color drop down list.
Comment`	Allows you to specify a comment.	Enter the comment.
File Name	Allows you to upload the shared binary data object.	Click Browse and select the file.

Table 8: Global User Role Configuration Details (*continued*)

Option	Function	Your Action
Global Role Options > Global Terminal Services Role Options tab		
Citrix Client CAB File Name	Specifies the custom Citrix client file name.	Enter the file name.
Citrix Client CAB File Version	Specifies the custom Citrix version.	Enter the version.

Related Documentation

- [Creating Secure Access Role-Based Source IP Alias \(NSM Procedure\) on page 38](#)
- [Configuring Secure Access General Session Options \(NSM Procedure\) on page 39](#)
- [Creating and Applying a Secure Access Device Template on page 29](#)
- [Verifying Imported Device Configurations on page 19](#)

Creating Secure Access Role-Based Source IP Alias (NSM Procedure)

To direct traffic to specific sites based on roles, you can define a source IP alias for each role. You use these aliases to configure virtual ports you define for the internal interface source IP address. A back-end device can then direct end-user traffic based on these aliases, as long as you configure the back-end device, such as a firewall, to expect the aliases in place of the internal interface source IP address. This capability enables you to direct various end users to defined sites based on their roles, even though all of the end-user traffic has the same internal interface source IP address.



NOTE: You must define virtual ports to take advantage of the role-based source IP aliases.

To specify a source IP alias for the role:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure user roles.
2. Click the **Configuration** tab, and select **Users > User Roles**. The corresponding workspace appears.
3. Click the **New** button and the New dialog box appears.
4. Add or modify settings on the **General > VLAN/Source IP** as specified in [Table 9 on page 39](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 9: IP Alias Configuration Details

Option	Function	Your Action
VLAN	Specifies role-based source IP aliases. If you want to direct traffic to specific sites based on roles, you can define a source IP alias for each role.	Select the VLAN you want to use from the VLAN list, if you have defined VLAN ports on your system. NOTE: If an end user is mapped to multiple roles and the Secure Access device merges roles, the Secure Access device associates the source IP address configured for the first role in the list with the merged role.
Select Source IP	Configures virtual ports you define for the internal interface source IP address.	Select a source IP address from the list. NOTE: You can specify the same source IP address for multiple roles. You cannot specify multiple source IP addresses for one role.

Related Documentation

- [Configuring Secure Access General Session Options \(NSM Procedure\) on page 39](#)
- [Creating and Configuring Secure Access Device Administrator Roles \(NSM Procedure\) on page 43](#)
- [Creating and Applying a Secure Access Device Template on page 29](#)
- [Verifying Imported Device Configurations on page 19](#)

Configuring Secure Access General Session Options (NSM Procedure)

To specify session time limits, roaming capabilities, session and password persistency, request follow-through options, and idle timeout application activity, follow these steps:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure user roles.
2. Click the **Configuration** tab, and select **Users > User Roles**. The corresponding workspace appears.
3. Click the **New** button and the New dialog box appears.
4. Click **General > Session Options** to add or modify settings as specified in [Table 10 on page 40](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modification.

Table 10: Session Options Configuration details

Option	Function	Your Action
General > Session Options tab		
Idle Timeout	Specifies the number of minutes a nonadministrative user session may remain idle before ending. The minimum is five minutes. The default idle session limit is 10 minutes, which means that if a user's session is inactive for 10 minutes, the Secure Access device ends the user session and logs the event in the system log (unless you enable session timeout warnings described later).	Enter the session length in minutes.
Max. Session Length	Specifies the number of minutes an active nonadministrative user session may remain open before ending. The minimum is six minutes. The default time limit for a user session is 60 minutes, after which the Secure Access device ends the user session and logs the event in the system log. During an end-user session, prior to the expiration of the maximum session length, the Secure Access device prompts the user to reenter authentication credentials, which avoids the problem of terminating the user session without warning.	Enter the heartbeat interval in seconds.
Reminder Time	Specifies when the Secure Access device should prompt nonadministrative users, warning them of an impending session or idle timeout. Specify in number of minutes before the timeout is reached.	Enter the Reminder Time in minutes.

Table 10: Session Options Configuration details (*continued*)

Option	Function	Your Action
Enable session timeout warning	Enables users to take the appropriate action when they are close to exceeding their session limits or idle timeouts, helping them to save any in-progress form data that would otherwise be lost. Users approaching the idle timeout limit are prompted to reactivate their session. Users approaching the session time limit are prompted to save data.	Select Enable session timeout warning to notify nonadministrative users when they are about to reach a session or idle timeout limit.
Display sign-in page on max session time out	Displays a new browser sign-in page to the end user when their session times out. This option appears only when you select Enable session timeout warning .	Select Display sign-in page on max session time out .
Roaming session	<p>Allows users to enable, limit, or disable the roaming session.</p> <p>A roaming user session works across source IP addresses, which allows mobile users (laptop users) with dynamic IP addresses to sign in to the Secure Access device from one location and continue working from another. Disable this feature to prevent users from accessing a previously established session from a new source IP address. This helps protect against an attack spoofing a user's session, provided the hacker was able to obtain a valid user's session cookie.</p> <p>Users may sign in from one IP address and continue using their sessions with another IP address as long as the new IP address is within the same subnet.</p> <p>Users who sign in from one IP address may not continue an active Secure Access device session from another IP address; user sessions are tied to the initial source IP address.</p>	<p>Select a roaming session option from the drop-down list:</p> <ul style="list-style-type: none"> • Enabled—Enables roaming user sessions for users mapped to this role. • Limit to subnet—Limits the roaming session to the local subnet specified in the Netmask box. • Disabled—Disables roaming user sessions for users mapped to this role.

Table 10: Session Options Configuration details (*continued*)

Option	Function	Your Action
Roaming netmask	Specifies the roaming netmask.	Enter a roaming netmask address.
Persistent session	Enables users to write the Secure Access device session cookie to the client hard disk so that the user's Secure Access device credentials are saved for the duration of the Secure Access device session.	Select Enabled from the drop-down list.
Persistent password caching	<p>Enables users to allow cached passwords to persist across sessions for a role.</p> <p>The Secure Access device supports the NT LAN Manager (NTLM) authentication protocol and HTTP Basic Authentication and supports servers that are set up to accept both NTLM and anonymous sign-in. The Secure Access device caches NTLM and HTTP Basic Authentication passwords provided by users so that the users are not repeatedly prompted to enter the same credentials used to sign in to the Secure Access device server or another resource in the NT domain. By default, the Secure Access device server flushes cached passwords when a user signs out.</p>	<p>Select Enabled from the drop-down list.</p> <p>You can delete cached passwords through the Advanced Preferences page. After the end user logs in to the Secure Access device, click Preferences and then click the Advanced tab.</p>
Browser request follow-through	Enables users to allow the Secure Access device to complete a user request made after an expired user session after the user reauthenticates.	Select Enabled form the drop-down list.
Idle timeout application activity	Enables users to ignore activities initiated by Web applications (such as polling for e-mails) when determining whether a session is active.	<p>Select Enabled form the drop-down list.</p> <p>If you disable this option, periodic ping or other application activity may prevent an idle timeout.</p>
Enable Upload Logs	Enables users to transmit (upload) client logs to the Secure Access device.	Select the Enable Upload Logs .

Related Documentation

- [Creating and Configuring Secure Access Device Administrator Roles \(NSM Procedure\) on page 43](#)
- [Creating Secure Access Role-Based Source IP Alias \(NSM Procedure\) on page 38](#)
- [Verifying Imported Device Configurations on page 19](#)
- [Creating and Applying a Secure Access Device Template on page 29](#)

Creating and Configuring Secure Access Device Administrator Roles (NSM Procedure)

An administrator role specifies Secure Access device management functions and session properties for administrators who map to the role. You can customize an administrator role by selecting the Secure Access device feature sets and user roles that members of the administrator role are allowed to view and manage. You can create and configure administrator roles through the Delegated Admin Roles page.



NOTE: To create individual administrator accounts, you must add the users through the appropriate authentication server (not the role). For example, to create an individual administrator account, you may use settings in the **Authentication > Auth. Servers > Administrators > Users** page of the admin console.

To create an administrator role:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure administrator role.
2. Click the **Configuration** tree tab, and select **Administrators > Admin Roles**.
3. Click the **New** button and the New dialog box appears.
4. Click **General > Overview** to add or modify settings as specified in [Table 11 on page 43](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 11: Administrator Role Configuration Details

Option	Function	Your Action
General > Overview tab		
Name	Specifies a unique name for the administrator role.	Enter a name.
Description	Describes the administrator role.	Enter a brief description for the administrator role.

Table 11: Administrator Role Configuration Details (*continued*)

Option	Function	Your Action
Session Options	Specifies the maximum session length, roaming capabilities, and session persistence.	Select General > Session Options to apply the settings to the role.
UI Options	Specifies customized settings for the Secure Access device welcome page for Odyssey Access Client users mapped to this role.	Select General > UI Options to apply the settings to the role.
Delegated Users Settings > Roles > Delegate User Roles		
Administrators can manage ALL roles	Specifies whether the administrator can manage all roles.	Select the user roles in the Non-members list and click Add if you only want to allow the administrator role to manage selected user roles
Access	Specifies which user role pages the delegated administrator can manage.	Select an access option from the drop-down list. <ul style="list-style-type: none"> • Select Write All to specify that members of the administrator role can modify all user role pages. • Select Custom Settings to allow you to pick and choose administrator privileges (Deny, Read, or Write) for the individual user role pages.
Delegated Users Settings > Roles > Delegate As Read-Only Role		
Administrator can view (but not modify) ALL roles	Allows the administrator to view the user roles, but not manage.	Select the user role that you want to allow the administrator to view. <p>NOTE: If you specify both write access and read-only access for a feature, the Secure Access device grants the most permissive access.</p>
Delegated Users Settings > Realms > Delegate User Realms		
Administrator can manage ALL realms	Specifies whether the administrator can manage all user authentication realms.	Select the user realm. If you only want to allow the administrator role to manage selected realms, select those realms in the Members list and click Add .

Table 11: Administrator Role Configuration Details (*continued*)

Option	Function	Your Action
Access	Specifies which user authentication realms pages that the delegated administrator can manage.	<p>Select an access option from drop-down list.</p> <ul style="list-style-type: none"> Select Write All to specify that members of the administrator role can modify all user authentication realm pages. Select Custom Settings to allow you to pick and choose administrator privileges (Deny, Read, or Write) for the individual user authentication realm pages.
Delegated Users Settings > Realms > Delegate As Read-Only Realms		
Administrator can view (but not modify) ALL realms	Allows the administrator to view the user authentication realms, but not modify.	<p>Select the user authentication realms that you want to allow the administrator to view.</p> <p>NOTE: If you specify both write access and read-only access for an authentication realm page, the Secure Access device grants the most permissive access.</p>
Delegated Administrator Settings > Management of Admin roles		
Manage ALL admin roles	Manages all admin roles.	Select Delegated Administrator Settings > Management of Admin roles > Manage ALL admin roles to manage all the admin roles.
Allow Add/Delete admin roles	<p>Allows the security administrator to create administrator roles, even if the security administrator is not part of the Administrators role.</p> <p>NOTE: This option appears only when you enable the Manage All admin roles option.</p>	Select to allow the security administrator to add and delete admin roles.

Table 11: Administrator Role Configuration Details (*continued*)

Option	Function	Your Action
Access	<p>Indicates the level of access that you want to allow the security administrator role to set for system administrators.</p> <p>NOTE: This option appears only when you enable the Manage All admin roles option.</p>	<p>Select an access option:</p> <ul style="list-style-type: none"> • Deny All—Specifies that members of the security administrator role cannot see or modify any settings in the category. • Read All—Specifies that members of the security administrator role can view, but not modify, all settings in the category. • Write All—Specifies that members of the security administrator role can modify all settings in the category. • Custom Settings—Allows you to pick and choose security administrator privileges (Deny, Read, or Write) for the individual features within the category.
Delegated Administrator Settings > Management of Admin realms		
Manage ALL admin realms	Manages all admin realms.	Select Delegated Administrator Settings > Management of Admin realms > Manage ALL admin realms .
Allow Add/Delete admin realms	<p>Allows the security administrator to create and delete administrator realms, even if the security administrator is not part of the administrators role.</p> <p>NOTE: This option only appears when you choose to enable the Manage All admin realms.</p>	Select to allow the security administrator to add and delete admin realms.

Table 11: Administrator Role Configuration Details (*continued*)

Option	Function	Your Action
Access	<p>Indicates the level of realm access that you want to allow the security administrator role to set for system administrators for each major set of admin console pages.</p> <p>NOTE: This option appears only when you enable the Manage All admin realm option.</p>	<p>Select an access option:</p> <ul style="list-style-type: none"> • Deny All—Specifies that members of the security administrator role cannot see or modify any settings in the category. • Read All—Specifies that members of the security administrator role can view, but not modify, all settings in the category. • Select Write All—Specifies that members of the security administrator role can modify all settings in the category. • Select Custom Settings—Allows you to pick and choose security administrator privileges (Deny, Read, or Write) for the individual features within the category.

Delegated Resource Policies > All tab

Access	<p>Indicates the level of access that you want to allow the administrator role for each Resource Policies submenu.</p>	<p>Select an access option:</p> <ul style="list-style-type: none"> • Deny All—Specifies that members of the administrator role cannot see or modify any resource policies. • Read All—Specifies that members of the administrator role can view, but not modify, all resource policies. • Write All—Specifies that members of the administrator role can modify all resource policies. • Custom Settings—Allows you to pick and choose administrator privileges (Deny, Read, or Write) for each type of resource policy or for individual resource policies. <p>NOTE: The Web, File, SAM, Telnet SSH, Terminal Services, Network Connect, and Email Client tabs are enabled only when you select Custom Settings from the drop down list.</p>
--------	------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Table 11: Administrator Role Configuration Details (*continued*)

Option	Function	Your Action
Delegated Resource Policies > Web > File > SAM > Telnet SSH > Terminal Services > Network Connect		
Access	Allows you to pick and choose administrator privileges for each type of resource policy.	Select Deny or Read or Write access level for the type of resource.
Additional Access Policies	Allows you to specify access level to individual policy (For example, if you want to control access to a resource policy that controls access to www.google.com)	Select a resource policy.
Access	Allows you to pick and choose administrator privileges for each individual resource policy.	Select Read or Write access level for the policy.
Delegated Resource Policies > Email Client		
Access	Allows you to pick and choose administrator privileges (Deny, Read, or Write) for the policy.	Select Deny or Read or Write access level for the.
Delegated Resource Profiles > All tab		

Table 11: Administrator Role Configuration Details (*continued*)

Option	Function	Your Action
Access	Indicate the level of access that you want to allow the administrator role for each Resource Profiles.	<p>Select an access option:</p> <ul style="list-style-type: none"> • Deny All—Specifies that members of the security administrator role cannot see or modify any settings in the category. • Read All—Specifies that members of the security administrator role can view, but not modify, all settings in the category. • Write All—Specifies that members of the security administrator role can modify all settings in the category. • Custom Settings—Allows you to pick and choose security administrator privileges (Deny, Read, or Write) for the individual features within the category. <p>NOTE: The Web, File, SAM, Telnet SSH, and Terminal Services tabs are enabled only when you select Custom Settings from the drop down list.</p>
Delegated Resource Profiles > Web > File > SAM > Telnet SSH > Terminal Services		
Access	Allows you to pick and choose administrator privileges for each type of resource profiles.	Select Deny or Read or Write access level for the type of resource.
Additional Access Profiles	Allows you to specify access level to individual profiles (For example, if you want to control access to a resource profiles that controls access to www.google.com).	Select the resource profile for which you want to provide a custom access level, and click Add .
Access	Allows you to pick and choose administrator privileges (Deny, Read, or Write) for the profiles.	Select Read or Write access level for the profiles.

Related Documentation

- [Configuring Access Options using Remote Access Mechanisms Overview on page 65](#)
- [Configuring Secure Access General Session Options \(NSM Procedure\) on page 39](#)
- [Creating and Applying a Secure Access Device Template on page 29](#)

- [Verifying Imported Device Configurations on page 19](#)

CHAPTER 7

Configuring Terminal Services Using Remote Access Mechanism

- [Terminal Services Overview on page 51](#)
- [Configuring Terminal Services on a Secure Access Device User Role \(NSM Procedure\) on page 52](#)
- [Terminal Services User Experience on page 61](#)
- [Terminal Services Execution on page 62](#)

Terminal Services Overview

You can use the Terminal Services feature to enable a terminal emulation session on a Windows terminal server, Citrix NFuse server, or Citrix Metaframe server. You can also use this feature to deliver the terminal services through the Secure Access device, eliminating the need to use another Web server to host the clients.



NOTE: The device supports several mechanisms for intermediating traffic between a Citrix server and client, including the Terminal Services, JSAM, WSAM, Network Connect, and hosted Java applets features.

Related Documentation

- [Terminal Services User Experience on page 61](#)
- [Terminal Services Execution on page 62](#)
- [Configuring Terminal Services on a Secure Access Device User Role \(NSM Procedure\) on page 52](#)

Configuring Terminal Services on a Secure Access Device User Role (NSM Procedure)

Use the Terminal Services feature to enable terminal emulation sessions on a Windows terminal server, Citrix NFuse server, or Citrix Metaframe server.

To configure terminal services on a user role:

1. In the navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure a terminal services option.
2. Click the **Configuration** tab. Select **Users > User Roles**.
3. Click the **New** button. The New dialog box appears.
4. Add or modify settings as specified in [Table 12 on page 52](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 12: User Role Terminal Services Configuration Details

Option	Function	Your Action
Terminal Services > Terminal Services Sessions tab		
Name	Specifies the name for the terminal services session bookmark.	Enter the name.
Description	Specifies the description for the terminal services session bookmark.	Enter the description.
Auto-launch	Enables the Secure Access device to automatically launch the resource for the user when the user signs into the Secure Access device.	Select the Auto Launch check box to enable this feature.

Table 12: User Role Terminal Services Configuration Details (*continued*)

Option	Function	Your Action
Type	Allows you to specify the type of user session you want to create.	<p>Select one of the following session type:</p> <ul style="list-style-type: none"> • Windows Terminal Services—Enables a terminal session to a Windows Terminal Server. • Citrix using default ICA—Enables a terminal services session to a Citrix Metaframe server. • Citrix using custom ICA file—Enables a terminal services session to a Citrix Metaframe or NFuse server governing a Citrix server farm.
Terminal Services > Terminal Services Sessions tab > Type > Windows Terminal Services > Settings tab		
Username	Specifies the username that the Secure Access device should pass to the terminal server.	<p>You can enter a static username or a variable.</p> <p>NOTE: Enter the <username> variable to pass the username stored in the Secure Access device's primary authentication server. Or use the following syntax to submit the username for the secondary authentication server: <username@Secondary ServerName> or <username[2]>.</p>
Password Type	Allows you to specify a static password or select a variable password if you want to use the password stored in the Secure Access device's primary or secondary authentication server.	Select either Variable Password or Explicit Password .
Variable Password	Specifies the SSO variable password that the Secure Access device uses to validate sign-in credentials.	Enter the variable password.
Explicit Password	Specifies the explicit SSO password that the Secure Access device uses to validate sign-in credentials.	Enter the explicit password.

Table 12: User Role Terminal Services Configuration Details (*continued*)

Option	Function	Your Action
Terminal Services > Terminal Services Sessions > Type > Windows Terminal Services > Start Application		
Launch Seamless Window	Allows you to have the Windows application server manage the display of the application.	Select the Launch Seamless Window check box to enable this feature.
Path to application	Specifies where the application's executable file resides on the terminal server in the Path to application box (visible only when you clear Launch seamless window).	Specify the path.
Working directory	Specifies where the terminal server should place working files for the application in the Working directory box.	Specify the directory.
Terminal Services > Terminal Services Sessions > Type > Windows Terminal Services > Connect Devices tab		
Connect drives	Allows you to connect the user's local drive to the terminal server, enabling the user to copy information from the terminal server to his local client directories.	Select the Connect drives check box to enable this feature.
Connect printers	Allows you to connect the user's local printers to the terminal server, enabling the user to print information from the terminal server to his local printer.	Select the Connect printers check box to enable this feature.
Connect COM Ports	Allows you to connect the user's COM ports to the terminal server, allowing communication between the terminal server and the devices on his serial ports.	Select the Connect COM Ports check box to enable this feature.
Allow Clipboard Sharing	Enables you to allow the contents of the clipboard to be shared between the user's host computer and the terminal server.	Select the Allow Clipboard Sharing check box to enable this feature.
Connect smart cards	Enables you to allow users to use smart cards to authenticate their remote desktop sessions.	Select the Connect smart cards check box to enable this feature.

Table 12: User Role Terminal Services Configuration Details (*continued*)

Option	Function	Your Action
Sound Options	Allows you to specify the sound options.	<p>Select one of the following options from drop-down list:</p> <ul style="list-style-type: none"> • Disable Sound Options—Allows you to disable the sound option. • Bring to this computer—Allows you to redirect audio to the local computer. • Leave at remote computer—Allows you to play the audio only at the server.
Terminal Services > Terminal Services Sessions > Type > Windows Terminal Services > Connection tab		
Host	Specifies the hostname or IP address of the Windows terminal server.	Enter the hostname or IP address.
Client Port	Allows you to specify the client port on which the user client communicates to the terminal server.	Enter the client port.
Server Port	Allows you to specify the server port on which terminal server listens to the user client.	Enter the server port.
Screen Size	Allows you to change the size of the terminal services window on the user's workstation. (By default, the Secure Access device sets the window size to full screen.)	Select Full Screen, 800x600, 1024x768, or 1280x1024 from the drop-down list.
Color Depth	Allows you to change the color-depth of the terminal session data. (By default, the Secure Access device sets the color depth to 8-bit.)	Select 8-bit, 15-bit, 16-bit, 24-bit, or 32-bit (True color) from the drop-down list.
Terminal Services > Terminal Services Sessions > Type > Windows Terminal Services > Experience Options tab		
Desktop background	Allows you to display a wallpaper background to users.	Select the Desktop background check box to enable this option.
Menu and window animation	Enables you to animate the movement of windows, menus, and lists.	Select the Menu and window animation check box to enable this option.

Table 12: User Role Terminal Services Configuration Details (*continued*)

Option	Function	Your Action
Bitmap Caching	Allows you to improve performance by minimizing the amount of display information that is passed over a connection.	Select the Bitmap Caching check box to enable this option.
Desktop Composition (RDP 6.0 onwards)	Allows you to make text smoother and easier to read. This option only works on Windows Vista computers running RDP clients that are version 6.0 or later.	Select the Desktop Composition (RDP 6.0 onwards) check box to enable this option.
Show contents of window while dragging	Specifies the contents of the Internet Explorer window while users move the windows on their desktops.	Select the Show contents of window while dragging check box to enable this option.
Themes	Allows users to set Windows themes in their terminal server windows.	Select the Show contents of window while dragging check box to enable this option.
Font smoothing (RDP 6.0 onwards)	Allows users to make text smoother and easier to read. This option only works on Windows Vista computers running RDP clients that are version 6.0 or later.	Select the Font smoothing (RDP 6.0 onwards) check box to enable this option.
Terminal Services > Terminal Services Sessions > Type > Citrix using default ICA file > Settings tab		
Username	Specifies the username that the Secure Access device should pass to the terminal server.	Enter a static username or a variable.
Password Type	Allows you to specify a static password or select a variable password.	Select either Variable Password or Explicit Password .
Variable Password	Specifies the SSO variable password that the Secure Access device uses to validate sign-in credentials.	Enter the variable password.
Explicit Password	Specifies the static SSO password that the Secure Access device uses to validate sign-in credentials.	Enter the static password.
Terminal Services > Terminal Services Sessions > Type > Citrix using default ICA file > Connection tab		

Table 12: User Role Terminal Services Configuration Details (*continued*)

Option	Function	Your Action
Host	Specifies the hostname or IP address of the Metaframe terminal server.	Enter the hostname or IP address.
Client Port	Specify the client port on which the user client communicates to the terminal server.	Enter the client port.
Server Port	Specifies the server port on which the terminal server listens to the user client.	Enter the server port.
Screen Size	Allows you to change the size of the terminal services window on the user's workstation. (By default, the Secure Access device sets the window size to full screen.)	Select Full Screen, 800x600, 1024x768, or 1280x1024 from the drop-down list.
Color Depth	Allows you to change the color-depth of the terminal session data. (By default, the Secure Access device sets the color depth to 8-bit.)	Select 8-bit, 15-bit, 16-bit, 24-bit, or 32-bit (True Color) from the drop-down list.
Terminal Services > Terminal Services Sessions > Type > Citrix using default ICA file > Start Application tab		
Path to application	Specifies where the application's executable file resides on the terminal server.	Enter the path.
Working directory	Specifies where the terminal server should place working files for the application.	Enter the path.
Terminal Services > Terminal Services Sessions > Type > Citrix using default ICA file > Session Reliability tab > Connect Devices tab		
Connect drives	Allows user to access local drives through the terminal session.	Select the Connect drives check box to enable this feature.
Connect printers	Allows user to access local printers through the terminal session.	Select the Connect printers check box to enable this feature.
Connect COM Ports	Allows user to access local COM ports through the terminal session.	Select the Connect COM Ports check box to enable this feature.
Terminal Services > Terminal Services Sessions > Type > Citrix using default ICA file > Session Reliability tab		

Table 12: User Role Terminal Services Configuration Details (*continued*)

Option	Function	Your Action
Session Reliability and Auto-client reconnect	Allows active ICA sessions to remain on the user's screen when network connectivity is interrupted.	Select the Session Reliability and Auto-client reconnect check box to enable this feature.
Port to be enabled	Allows you to enter the port to use.	Enter the port number.
Terminal Services > Terminal Services Sessions tab > Type > Citrix using custom ICA file		
Username	Specifies a unique name for the resource profile. (This name becomes the default session bookmark's name.)	Enter the username.
Password Type	Allows you to specify a static password or select a variable password.	Select either Variable Password or Explicit Password .
Variable Password	Specifies the SSO variable password that the Secure Access device uses to validate sign-in credentials.	Enter the variable password.
Explicit Password	Specifies the explicit SSO password that the Secure Access device uses to validate sign-in credentials.	Enter the static password.
Custom ICA File	Allows you to specify the ICA file that contains the session parameters that you want use in the Custom ICA File box. Note that you may download and customize the following ICA files from the Secure Access device.	Enter the ICA file or Click Browse and select the ICA File.
Custom ICA Filename	Specifies the ICA filename.	Enter a name.
Terminal Services > Options > Citrix Delivery tab		

Table 12: User Role Terminal Services Configuration Details (*continued*)

Option	Function	Your Action
Citrix Client Delivery Method	Enables you to specify where the Secure Access device should obtain the ICA client to download to users' systems.	<p>Select one of the following from the drop-down list:</p> <ul style="list-style-type: none"> • Downloaded from the Citrix web site— The Secure Access device installs the latest version of the ICA client from the Citrix Web site. • Downloaded from the Secure Gateway—Use the Browse button to browse to the ICA client on your local network. • Downloaded from a URL—The Secure Access device installs the ICA client of your choice from the specified Web site. You must also specify the exact version number of the ICA client.
Citrix Client Download URL	<p>Specifies the URL used to fetch the Citrix Client.</p> <p>NOTE: The Citrix Client Download and Citrix Client Download Version boxes are displayed only when you select Downloaded from a URL option from the Citrix Client Delivery Method drop-down list.</p>	Enter the URL.
Citrix Client Download Version	Specifies the version to download.	Enter the version.
Terminal Services > Options > User Permissions tab		
User can add sessions	Enables users to define their own terminal session bookmarks and to enable users to access terminal servers through the Secure Access device browse bar on the Secure Access device home page.	Select the User can add sessions check box to enable this option.
Users can connect drives	Enables user to create bookmarks that connect their local drives to the terminal server, enabling users to copy information from the terminal server to their local client directories.	Select the Users can connect drives check box to enable this option.

Table 12: User Role Terminal Services Configuration Details (*continued*)

Option	Function	Your Action
User can connect COM ports	Enables users to create bookmarks that connect their COM ports to the terminal server, allowing communication between the terminal server and the devices on their serial ports.	Select the User can connect COM ports check box to enable this option.
User can connect printers	Enables users to create bookmarks that connect their local printers to the terminal server, enabling users to print information from the terminal server to their printers.	Select the User can connect printers check box to enable this option.
Allow clipboard Sharing	Enables users to create bookmarks that share the contents of the clipboard between the user's host computer and the terminal server.	Select the Allow Clipboard Sharing check box to enable this option.
User can connect smart cards	Allows users to use smart card readers connected to their system for authenticating their remote desktop session.	Select the User can connect smart cards check box to enable this option.
User can connect sound devices	Allows users to redirect audio from the remote desktop session to their local system.	Select the User can connect sound devices check box to enable this option.
Terminal Services > Options > Experience Options tab		
Desktop background	Displays your current wallpaper setting.	Select the Desktop background check box to enable this option.
Menu and window animation	Allows you to animate the movement of windows, menus, and lists.	Select the Menu and window animation check box to enable this option.
Bitmap Caching	Allows you to improve the performance by minimizing the amount of display information that must be passed over a connection.	Select the Bitmap Caching check box to enable this option.
Desktop Composition (RDP 6.0 onwards)	Specifies that the drawing is redirected to video memory, which is then rendered into a desktop image.	Select the Desktop Composition (RDP 6.0 onwards) check box to enable this option.

Table 12: User Role Terminal Services Configuration Details (*continued*)

Option	Function	Your Action
Show contents of window while dragging	Specifies the contents of the Internet Explorer window while moving the window around your desktop.	Select the Show contents of window while dragging check box to enable this option.
Themes	Allows Windows themes to be set in the terminal server window.	Select the Themes check box to enable this option.
Font smoothing (RDP 6.0 onwards)	Allows you to read the text smoother and easier. This option only works on Windows Vista computers running RDP clients that are version 6.0 or later.	Select the Font Smoothing (RDP 6.0 onwards) check box to enable this option.

- Related Documentation**
- [Terminal Services User Experience on page 61](#)
 - [Terminal Services Execution on page 62](#)

Terminal Services User Experience

From an enduser perspective, accessing secured terminal services resources through the Secure Access device is simple. When you enable the Terminal Services feature for a user role, the enduser needs to perform the following tasks as described in [Table 13 on page 61](#).

Table 13: Terminal Services User Experience

Options	Your Action
Specify the resource that the user wants to access	Click a link to enter the required resource or enter the resource in the device browse bar. Or, Alternatively, enable auto-launch for a bookmark and the device automatically launches the resource when you sign in to the device.
Enter credentials for the resource	Access a resource so that the device prompts to enter the username and password (if required by the resource). Alternatively, enable SSO and the device automatically sends this information to the resource without prompting for username and password. Once the resource verifies the credentials, the device launches the resource.



NOTE: The following options in the New Terminal Services Sessions window do not apply to remote desktops launched in the following order:

- Client port
- Authentication settings
- Start application settings
- Connect Devices settings
- Display Settings

Related Documentation

- [Terminal Services Execution on page 62](#)
- [Configuring Terminal Services on a Secure Access Device User Role \(NSM Procedure\) on page 52](#)

Terminal Services Execution

When a user tries to access a terminal services resource, the device completes the steps in the page to initiate and intermediate the terminal services session as described in [Table 14 on page 62](#).

Table 14: Terminal Services User Experience

Options	Your Action
The device checks for a Java client	<p>Ensure that you have an RDP client on the system (to access a Windows terminal server) or an ICA client (to access a Citrix Metaframe server or server farm). This enables a terminal service session. The RDP clients come in both Windows and Java versions and enables you to run an application on the server while only transmitting keyboard, mouse, and display information over the network.</p> <p>The device enables to upload a Java version of the RDP or ICA client through a terminal service resource profile (but not role). If you have uploaded a client to the device and specified that the device always use it to run your users' terminal sessions, the device launches the specified Java client.</p>
If necessary, the device checks for a Windows client (Citrix only)	Ensure that you have uploaded a Java client to the device, else the device checks for a Windows version of the ICA client. If the device cannot find a Windows ICA client, it installs the version you specified in the Users > User Roles > Role > Terminal Services > Options page.
The device checks for the terminal services proxy	Ensure that you have a Juniper Windows Terminal Services proxy on your system or a Juniper Networks Citrix Terminal Services proxy, to intermediate a Windows or Citrix session. The device checks for the appropriate proxy on the user's computer, and if it cannot find it, the system installs a new one. Depending on the user's rights, the device either uses an ActiveX component or Java component to install the proxy.
The proxy tries to invoke the Windows client	Ensure that the device has confirmed that a proxy is installed on the user's computer. This enables the proxy to attempt to invoke the Windows RDP or ICA client. If successful, the client initiates the user's terminal services session and the proxy intermediates the session traffic.

Table 14: Terminal Services User Experience (*continued*)

Options	Your Action
The proxy tries to invoke the Java client	<p>Ensure that you have uploaded a Windows client to the device through the terminal services resource profile. If the Windows client is not present on the user's machine (for instance, because it was deleted or because the user does not have the proper privileges to install it), the device uses the uploaded Java applet to launch the session.</p> <p>As part of the installation, the device prompts you whether if the you want to always use the Java client or only for this session. The device then stores the user's preference as a persistent cookie. Once the Java client is installed, the client initiates the user's terminal services session and the proxy intermediates the session traffic.</p>



NOTE: The following options in the New Terminal Services Sessions window do not apply to remote desktops launched in the following order:

- Client port
- Authentication settings
- Start application settings
- Connect Devices settings
- Display Settings

**Related
Documentation**

- [Terminal Services User Experience on page 61](#)
- [Configuring Terminal Services on a Secure Access Device User Role \(NSM Procedure\) on page 52](#)

CHAPTER 8

Configuring Access Options using Remote Access Mechanisms

- [Configuring Access Options using Remote Access Mechanisms Overview on page 65](#)
- [Configuring File Rewriting on a Secure Access Device User Role \(NSM Procedure\) on page 66](#)
- [Configuring Network Connect on a Secure Access Device User Role \(NSM Procedure\) on page 69](#)
- [Configuring Secure Application Manager on a Secure Access Device User Role \(NSM Procedure\) on page 73](#)
- [Configuring Secure Meeting on a Secure Access Device User Role \(NSM Procedure\) on page 78](#)
- [Configuring Web Rewriting on a Secure Access Device User Role \(NSM Procedure\) on page 84](#)
- [Configuring Telnet/SSH on a Secure Access Device User Role \(NSM Procedure\) on page 89](#)

Configuring Access Options using Remote Access Mechanisms Overview

This chapter contains the following information about configuring access in NSM to various applications, servers, and other resources using remote access mechanisms.. When you enable an access feature, make sure to create corresponding resource policies. To enable access features See “Configuring Secure Access Device User Roles (NSM Procedure).”

For instance, if you want to secure access to Microsoft Outlook, you can use the Secure Application Manager (SAM). The Secure Application Manager intermediates traffic to client/server applications including Microsoft Outlook, Lotus Notes, and Citrix. Or, if you want to secure access to your company Intranet, you can use the Web rewriting feature. This feature uses the Secure Access devices Content Intermediation Engine to intermediate traffic to Web-based applications and Web pages.

However, you can only access features through a user role if you are licensed for the feature. For instance, if you are using an SA-700 appliance and have not purchased a Core Clientless Access upgrade license, you cannot enable Web rewriting for a user role.

This chapter contains the following information about the access options using remote mechanisms in NSM:

- [Configuring File Rewriting on a Secure Access Device User Role \(NSM Procedure\) on page 66](#)
 - [Configuring Network Connect on a Secure Access Device User Role \(NSM Procedure\) on page 69](#)
 - [Configuring Secure Application Manager on a Secure Access Device User Role \(NSM Procedure\) on page 73](#)
 - [Configuring Secure Meeting on a Secure Access Device User Role \(NSM Procedure\) on page 78](#)
 - [Configuring Web Rewriting on a Secure Access Device User Role \(NSM Procedure\) on page 84](#)
 - [Configuring Telnet/SSH on a Secure Access Device User Role \(NSM Procedure\) on page 89](#)
- Related Documentation**
- [Configuring File Rewriting on a Secure Access Device User Role \(NSM Procedure\) on page 66](#)
 - [Configuring Network Connect on a Secure Access Device User Role \(NSM Procedure\) on page 69](#)

Configuring File Rewriting on a Secure Access Device User Role (NSM Procedure)

A file resource profile controls access to resources on Windows server shares or UNIX servers.

To configure file rewriting on a user role:

1. In the navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure a file rewriting option.
2. Click the **Configuration** tab. Select **Users > User Roles**.
3. Click the **New** button. The New dialog box appears.
4. Add or modify settings as specified in [Table 15 on page 66](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 15: User Role File Rewriting Configuration Details

Option	Function	Your Action
Files > File Bookmarks > Windows Bookmarks tab		

Table 15: User Role File Rewriting Configuration Details (*continued*)

Option	Function	Your Action
Name	Specifies the bookmark name for the device's home page.	Enter a name.
Description	Specifies the description for the device's home page bookmark.	Enter a description.
Server	Specifies the server name for the bookmark.	Enter the server hostname or IP address.
Share	Specifies the share name for the bookmark.	Enter the share name.
Path	Specifies the path for restricting access.	Enter the path.
Appearance	Specifies the bookmark on a user's welcome page and when browsing network files.	Select an appearance option from the drop-down list: <ul style="list-style-type: none"> • Appear as bookmark on home and file browsing—The bookmark appears both on a user's welcome page and when browsing network files. • Appear in file browsing only—The bookmark appears only when browsing network files.
Files > File Bookmarks > Unix Bookmarks tab		
Name	Specifies the device home page name of the bookmark.	Enter a name.
Description	Specifies the device home page description of the bookmark.	Enter a description.
Server	Specifies the server name for the bookmark.	Enter the server hostname or IP address.
Path	Specifies the path for the restricting access.	Enter the path to further restrict access.

Table 15: User Role File Rewriting Configuration Details (*continued*)

Option	Function	Your Action
Appearance	Specifies the bookmark on a user's welcome page and when browsing network files.	<p>Select an appearance option from the drop-down list:</p> <ul style="list-style-type: none"> • Appear as bookmark on home and file browsing—The bookmark appears both on a user's welcome page and when browsing network files. • Appear in file browsing only—The bookmark appears only when browsing network files.
Files > Windows network files options tab		
User can browse network file shares	Allows users to browse network file shares.	Select the User can browse network file shares check box to enable this feature.
Users can add bookmarks	Allows users to view and create bookmarks to resources on available Windows file shares.	Select the Users can add bookmarks check box to enable this feature.
Files > Unix network files options tab		
User can browse network file shares	Allows users to view and create bookmarks to resources on available UNIX file shares.	Select the User can browse network file shares check box to enable this feature.
User can add bookmarks	Allows users to add and create bookmarks to resources on available UNIX file shares.	Select the User can add bookmarks check box to enable this feature.
Allow automount shares	Allows users access to automount shares specified on an NIS server.	Select the Allow automount shares check box to enable this feature.

Related Documentation

- [Configuring Network Connect on a Secure Access Device User Role \(NSM Procedure\) on page 69](#)
- [Configuring Secure Application Manager on a Secure Access Device User Role \(NSM Procedure\) on page 73](#)

Configuring Network Connect on a Secure Access Device User Role (NSM Procedure)

The Network Connect option provides secure, SSL-based network-level remote access to all enterprise application resources using the Secure Access device over port 443.

To configure network connect on a user role:

1. In the navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure a user-role access option.
2. Click the **Configuration** tab. Select **Users > User Roles**.
3. Click the **New** button. The New dialog box appears.
4. Add or modify settings as specified in [Table 16 on page 69](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 16: User Role Network Connect Configuration Details

Option	Function	Your Action
Network Connect tab		

Table 16: User Role Network Connect Configuration Details (*continued*)

Option	Function	Your Action
Split Tunneling Modes	Allows you to enable split tunneling.	

Table 16: User Role Network Connect Configuration Details (*continued*)

Option	Function	Your Action
		<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> Disable Split Tunneling—When Network Connect successfully establishes a connection to the Secure Access device, the device removes any predefined local (client) subnet and host-to-host routes that might cause split-tunneling behavior. If any changes are made to the client's route table during an active Network Connect session, the Secure Access device terminates the session. Allow access to local subnet—The Secure Access device preserves the route on the client, retaining access to local resources such as printers. If needed, you can add entries to the client's route table during the Network Connect session. The Secure Access device does not terminate the session. This is the default option. Enable Split Tunneling—This option activates split-tunneling and requires you to specify the network IP address/netmask combinations. For the specified network IP address/netmask combinations, the Secure Access device handles traffic passed between the remote client and the corporate intranet. Enable Split Tunneling with route change monitor— This option retains access to local resources such as printers. Enable Split Tunneling with allowed access to local subnet—This option activates split-tunneling and preserves the route on the

Table 16: User Role Network Connect Configuration Details (*continued*)

Option	Function	Your Action
		client, retaining access to local resources such as printers.
Auto-launch Network Connect	Specifies whether or not Network Connect automatically launches when an authenticated user maps to one or more roles that enable Network Connect sessions.	Select the Auto-Launch Network Connect check box to enable this feature.
Auto-Uninstall Network Connect	Specifies whether or not Network Connect uninstalls itself from the remote client when a user signs-out of the Network Connect session.	Select the Auto-Uninstall Network Connect check box to enable this feature.
Enable TOS Bits Copy	Specifies that Network Connect to copy IP TOS bits from the inner IP packet header to the outer IP packet header.	Select the Enable TOS Bits Copy check box to enable this feature.
Multicast	Specifies whether or not you want Network Connect to operate in multicast mode.	Select the Multicast check box to enable this feature.
Install GINA with Network Connect	Additionally installs GINA on a client system when you install Network Connect.	Select the Install GINA with Network Connect check box to enable this feature.
GINA Options	Specifies whether or not to enable GINA installation for a role and specifies the GINA sign-in behavior.	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • Require NC to start when logging into Windows (Note that this may require a reboot when NC is installed)—Automatically launches the Network Connect sign-in function at every Windows user sign-in. • Allow user to decide whether to start NC when logging into Windows—Allows the user to determine, at each Windows startup, whether or not to launch Network Connect after GINA installation.
Windows: Session start script location	Specifies the location of Network Connect start scripts for Windows.	Enter the start script location.

Table 16: User Role Network Connect Configuration Details (*continued*)

Option	Function	Your Action
Windows: Session end script location	Specifies the location of Network Connect end scripts for Windows.	Enter the end script location.
Skip if GINA Enabled	Bypasses the specified Windows session start script. The sign-in script may be identical to the specified Network Connect start script. This feature avoids executing the same script twice.	Select the Skip if GINA enabled check box to enable this feature.
Linux: Session start script location	Specifies the location of Network Connect start scripts for Linux.	Enter the start script location.
Linux: Session end script location	Specifies the location of Network Connect end scripts for Linux.	Enter the end script location.
Mac: Session start script location	Specifies the location of Network Connect start scripts for Macintosh.	Enter the start script location.
Mac: Session end script location	Specifies the location of Network Connect end scripts for Macintosh.	Enter the end script location.

Related Documentation

- [Configuring Secure Application Manager on a Secure Access Device User Role \(NSM Procedure\) on page 73](#)
- [Configuring Secure Meeting on a Secure Access Device User Role \(NSM Procedure\) on page 78](#)

Configuring Secure Application Manager on a Secure Access Device User Role (NSM Procedure)

The Secure Application Manager (SAM) option provides secure, application-level remote access to enterprise servers from client applications.

To configure SAM option on the user role:

1. In the navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure a Secure Application Manager on a user-role access option.
2. Click the **configuration** tab. Select **Users > User Roles**.
3. Click the **New** button. The New Dialog box appears.

4. Add or modify settings as specified in [Table 17 on page 74](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 17: User Role SAM Configuration Details

Option	Function	Your Action
SAM > JSAM Applications tab		
Name	Displays the application name in the Client Application Sessions area of the Secure Access device end-user home page.	Enter the name of the application.
Description	Displays the description in the Client Application Sessions area of the Secure Access device end-user home page.	Enter the description.
Type	Specifies the applications for which JSAM secures traffic.	Select one of the following option Custom , Citrix NFuse , Lotus Notes , Microsoft Outlook/Exchange , NetBIOS file browsing from the drop-down list.
Type > Custom		
Server Hostname or IP	Specifies the DNS name of the server or the server IP address.	Enter the DNS name or the IP address.
Server Port	Specifies the port on which the remote server listens for client connections.	Enter the port number.
Localhost IP	Specifies a static address for JSAM to listen on loopback address for client requests to network application servers.	Enter a static loopback address.
Client Port	Specifies the port on which JSAM should listen for client application connections.	Enter the port number.
Allow Secure Application Manager to dynamically select an available port if the specified client port is taken	Allows JSAM to select an available port when the client port you specify is taken.	Select the Allow Secure Application Manager to dynamically select an available port if the specified client port is taken check box to enable this feature.
Type > Citrix NFuse		

Table 17: User Role SAM Configuration Details (*continued*)

Option	Function	Your Action
Maximum Citrix Sessions	Specifies the maximum number of client sessions.	Enter the number.
New Allowed Citrix Ports	Specifies the ports on which the Metaframe servers listen.	Enter the port number.
Type > Microsoft Outlook/Exchange		
New Application Servers	Specifies the application servers for client application connections.	Enter the server name.
Type > NetBIOS file browsing		
New Application Servers	Specifies the application servers for client application connections.	Enter the server name.
SAM > WSAM Applications tab		
Name	Displays the application name in the Client Application Sessions area of the Secure Access device end-user home page.	Enter the name of the application.
Description	Displays the description in the Client Application Sessions area of the Secure Access device end-user home page.	Enter the description.
Applications	Specifies the applications for which WSAM secures traffic.	Select one of the following option Citrix , Lotus Notes , Microsoft Outlook/Exchange , NetBIOS file browsing or Custom from the Applications drop-down list.
SAM > WSAM Allowed Servers tab		
Name	Displays the application name in the Client Application Sessions area of the Secure Access device end-user home page.	Enter the name of the application.
Description	Displays the description in the Client Application Sessions area of the Secure Access device end-user home page.	Enter the description.
Server	Allows you to specify the server's hostname (the wild cards '*' or '?' are accepted) or an IP/netmask pair.	Enter the server's hostname.

Table 17: User Role SAM Configuration Details (*continued*)

Option	Function	Your Action
Ports	Allows you to specify multiple ports for a host as separate entries.	Enter the port numbers.
SAM > WSAM Bypass Applications tab		
Name	Displays the application name in the Client Application Sessions area of the Secure Access device in the end-user home page.	Enter the name of the application.
Description	Displays the description in the Client Application Sessions area of the Secure Access device in the end-user home page.	Enter the description.
Application	Specifies the application for which WSAM client does not secure traffic.	Enter the application name.
Path	Allows you to provide an absolute path to the application.	Enter the path.
SAM tab > Options tab		
Auto-launch Secure Application Manager	Enables the Secure Access device to automatically launch the Secure Application Manager when a user signs in. If you do not select this option, users must manually start the Secure Application Manager from the Client Applications Sessions Area of the Secure Access device end-user home page.	Select the Auto-launch Secure Application Manager check box to enable this feature.
Auto-uninstall Secure Application Manager	Enables the Secure Access device to automatically uninstall the Secure Application Manager after user signs off.	Select the Auto-uninstall Secure Application Manager check box to enable this feature.

Table 17: User Role SAM Configuration Details (*continued*)

Option	Function	Your Action
Prompt for username and password for intranet sites	Allows the Secure Access device to prompt users to enter their sign-in credentials before connecting to sites on their internal network. This option changes Internet Explorer's intranet zone setting so that Internet Explorer prompts the user for network sign-in credentials whenever the user wants to access an intranet site.	Select the Prompt for username and password for intranet sites check box to enable this feature.
Auto-upgrade Secure Application Manager	Enables the Secure Access device to automatically download the Secure Application Manager to a client machine when the version of Secure Application Manager on the Secure Access device is newer than the version installed on the client.	Select the Auto-upgrade Secure Application Manager check box to enable this feature.
Session start script	Enables the Secure Access device to run a batch, application, or Win32 service file when the WSAM session starts.	Enter the name and path for the file.
Session end script	Enables the Secure Access device to run a batch, application, or Win32 service file when the WSAM session ends.	Enter the name and path for the file.
User can add applications	Enables user to add applications.	Select the User can add applications check box to enable this feature.
Automatic host-mapping	Allows the Secure Application Manager to edit the Windows PC hosts file and replaces entries of Windows application servers with localhost. These entries are changed back to the original data when a user closes the Secure Application Manager.	Select the Automatic host-mapping check box to enable this feature.

Table 17: User Role SAM Configuration Details (*continued*)

Option	Function	Your Action
Skip web-proxy registry check	Does not have JSAM check a user's registry for a Web proxy. Some users do not have permissions to look at their registries. If JSAM tries to look at their registries, then users see an error that they do not have permission. This option ensures that users do not see this message.	Select the Skip web-proxy registry check check box to enable this feature.
Auto-close JSAM window on sign-out	Enables JSAM to automatically close when a user signs out of the Secure Access device by clicking Sign Out in the Secure Access device browser window. JSAM continues to run if the user simply closes the browser window.	Select the Auto-close JSAM window on sign-out check box to enable this feature.

Related Documentation

- [Configuring Secure Meeting on a Secure Access Device User Role \(NSM Procedure\) on page 78](#)
- [Configuring Terminal Services on a Secure Access Device User Role \(NSM Procedure\) on page 52](#)
- [Configuring WSAM Resource Profile \(NSM Procedure\) on page 131](#)

Configuring Secure Meeting on a Secure Access Device User Role (NSM Procedure)

Secure Meeting allows Secure Access device users to securely schedule and hold online meetings among Secure Access device users and non-Secure Access device users. In meetings, users can share their desktops and applications with one another over a secure connection, allowing everyone in the meeting to instantaneously share electronic data onscreen. Meeting attendees can also securely collaborate online by remote-controlling one another's desktops and through text chatting using a separate application window that does not interfere with the presentation.

To configure secure meeting on a user role:

1. In the navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure secure meeting on a user role.
2. Click the **Configuration** tab. Select **Users > User Roles**.
3. Click the **New** button. The New dialog box appears.
4. Add or modify settings as specified in [Table 18 on page 79](#).
5. Click one:

- **OK**—Saves the changes.
- **Cancel**—Cancels the modifications.

Table 18: User Role Secure Meeting Configuration Details

Option	Function	Your Action
Meetings > Options > Meeting Types tab		
User cannot create meetings	Disables meeting creation and scheduling. NOTE: User can join the invited meetings even if you enable this option.	Select the User cannot create meetings check box to enable this feature.
Meeting Types	Specifies the type of meeting you want to provide users.	Select one of the following options from the drop-down list: <ul style="list-style-type: none"> • MySecureMeeting (users have a personal meeting URL)—Allows users to create personal meetings without having to schedule them ahead of time. • Standard meetings (users can create scheduled meetings)— Allows users to create scheduled meetings through the Meetings tab.
Users can create Scheduled meetings	Allows users to create scheduled meetings.	Select the Users can create Scheduled meetings check box to enable this feature.
Users can create Instant meetings	Allows users to create instant meetings.	Select the Meetings > Options > Meeting Types > Users can create Instant meetings check box to enable this feature.
Users can create Support meetings	Allows users to create two-person support meetings.	Select the Meetings > Options > Meeting Types > Users can create Support meetings check box to enable this feature.
Users can create additional meeting URLs under their personal URL	Allows users to create an additional meetingID.	Select the Meetings > Options > Meeting Types > Users can create additional meeting URLs under their personal URL check box to enable this feature.
Meetings > Options > Meeting Options tab		

Table 18: User Role Secure Meeting Configuration Details (*continued*)

Option	Function	Your Action
Authentication Requirements	Specifies the authentication restrictions that you want users to apply to the meetings that they create.	<p>Select one of the following types from the drop-down list:</p> <ul style="list-style-type: none">• Meeting password optional (more accessible)—Allows the meeting creator to decide whether or not the meeting requires a password to join.• Require meeting password (more secure)—Requires the meeting creator to either create a meeting password or use the one generated by Secure Meeting.• Require server-generated password (even more secure)—Requires the meeting creator to use the password generated by Secure Meeting.• Require secure gateway authentication (most secure)—Allows only invited users authenticated against the Secure Access device secure gateway to attend the meetings.

Table 18: User Role Secure Meeting Configuration Details (*continued*)

Option	Function	Your Action
Password Distribution	Specifies the distribution method that you want meeting creators to employ.	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • Do not display the password in the notification email (more secure)—Requires that meeting creators manually distribute the meeting password to invitees. • Display the password in the notification email (more accessible)—Automatically distributes the meeting password in the e-mail notification sent by Secure Meeting and displays the Secure Meeting tab in Microsoft Outlook calendar entries. • Allow the meeting creator to decide—Allows meeting creator to determine whether or not Secure Meeting and Microsoft Outlook should automatically distribute the meeting password to meeting invitees.
Attendee Names	Specifies whether you want Secure Meeting to display the names of attendees during a meeting.	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • Do not allow hiding of attendee names—Always displays the names of meeting attendees. • Allow meeting creator to hide attendee names—Allows the meeting creator to decide whether or not to display the names of meeting attendees. • Hide attendee names—Always hides the names of meeting attendees. <p>NOTE: When you select this option, Secure Meeting still exposes the names of the meeting conductor and presenter to other meeting attendees.</p>

Table 18: User Role Secure Meeting Configuration Details (*continued*)

Option	Function	Your Action
Secure Chat	Specifies whether or not you want to allow users to chat during their meetings.	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • Allow secure chat (more functional)—Enables chatting in the meetings that are created by users who map to this role. • Disable secure chat (more secure)—Disables chatting in the meetings that are created by users who map to this role. <p>NOTE: If you change this setting while a meeting is in progress (that is, after any user has joined the meeting), Secure Meeting does not apply the modified setting to the in-progress meeting.</p>
Allow users to download Secure Meeting for Outlook Plugin	Allows users to schedule secure meetings through Microsoft Outlook.	Select the Allow users to download Secure Meeting for Outlook Plugin check box to enable this feature.
Minimum length (characters)	Allows you to set the minimum character length for passwords.	Set the minimum character length for passwords.
Maximum length (character)	Allows you to set the maximum character length for passwords.	Set the maximum character length for passwords.
Password must have one or more digits	Requires passwords to have at least one digit.	Select the Password must have one or more digits check box to enable this feature.
Password must have one or more letters	Requires passwords to have at least one letter.	Select the Password must have one or more letters check box to enable this feature.
Password must have mix of UPPERCASE and lowercase letters	Requires all passwords to contain a mixture of upper- and lowercase letters.	Select the Password must have mix of UPPERCASE and lowercase letters check box to enable this feature.
Password must be different from username	Requires that the password cannot equal the username.	Select the Password must be different from username check box to enable this feature.

Table 18: User Role Secure Meeting Configuration Details (*continued*)

Option	Function	Your Action
Password Management	Allows you to prompt user to renew password after specific number of meetings.	Enter the number. NOTE: Enter <-1> to not renew the meeting password.
Remote Control	Specifies whether you want to allow meeting presenters to share control of their desktops and applications with other meeting attendees.	Select one of the following options from drop-down list: <ul style="list-style-type: none"> • Allow remote control of shared windows (more functional)—Allows the meeting presenter or conductor to pass control of the presenter's desktop and desktop applications to any of the meeting attendees, including non-Secure Access device users. • Disable remote control (more secure)—Allows Limited control of the meeting presenter's desktop and desktop applications exclusively to the presenter.
Meetings > Options > Meeting Policy Settings tab		
Limit number of simultaneous meetings	Allows you to specify the maximum number of meetings that may be held by at any given time by members of the role.	Select the Limit number of simultaneous meetings check box to enable this feature.
Limit number of simultaneous meeting attendees	Allows you to specify the maximum number of people who may simultaneously attend meetings scheduled by members of the role.	Select the Limit number of simultaneous meeting attendees check box to enable this feature.
Limit duration of meetings (minutes)	Allows you to specify a maximum duration (in minutes) that a meeting may run.	Select the Limit duration of meetings (minutes) to enable this feature.
Meetings > Auth Servers		
All Authentication Servers	Exports all authentication servers or selected authentication servers.	Select the ALL Authentication Servers check box to enable this feature.
Auth Servers with Access Privilege	Specifies whether the members of this role may access and search the authentication servers that they are currently authenticated against.	Select the authentication server and click Add .

Table 18: User Role Secure Meeting Configuration Details (*continued*)

Option	Function	Your Action
All Authentication Servers	Exports all authentication servers or selected servers to export.	Select ALL auth servers to export all authentication servers or SELECTED auth servers to specify which authentication servers to export.
Auth Servers With Search Privilege	Specifies additional authentication servers that members of this role may access and search.	Select the Auth Servers With Search Privilege check box to enable this feature.

Related Documentation

- [Configuring Terminal Services on a Secure Access Device User Role \(NSM Procedure\) on page 52](#)
- [Configuring Web Rewriting on a Secure Access Device User Role \(NSM Procedure\) on page 84](#)

Configuring Web Rewriting on a Secure Access Device User Role (NSM Procedure)

The Secure Access device Web rewriting feature enables you to intermediate Web URLs through the Content Intermediation Engine. You can intermediate URLs on the World Wide Web or on your corporate Intranet.

To configure Web rewriting on the user role:

1. In the navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure Web rewriting.
2. Click the **Configuration** tab. Select **Users > User Roles**.
3. Click the **New** button. The New dialog box appears.
4. Add or modify settings as specified in [Table 19 on page 84](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 19: User Role Web Rewriting Configuration Details

Option	Function	Your Action
Web > Web Bookmarks tab		
Name	Specifies the name for the device home page bookmark.	Enter a name.

Table 19: User Role Web Rewriting Configuration Details (*continued*)

Option	Function	Your Action
Description	Specifies the description for the device home page bookmark.	Enter a description.
Open New Window	Enables the Secure Access device to automatically open the web resource in a new browser window.	Select the Open New Window check box to enable this feature.
Do Not Display Address Bar	<p>Allows Web traffic through the Secure Access device by precluding users in the specified role from typing a new URL in the address bar.</p> <p>This option is displayed only when you enable the Open New Window option.</p>	Select the Do Not Display Address Bar check box to enable this feature.
Do Not Display Tool Bar	<p>Allows all Web traffic through the Secure Access device by precluding users in the specified role from typing a new URL in the tool bar.</p> <p>This option is displayed only when you enable the Open New Window option.</p>	Select the Do Not Display Tool Bar check box to enable this feature.
Bookmark Type	Allows you to create two types of bookmarks.	<p>Select one of the following option:</p> <ul style="list-style-type: none"> • Standard—Links the user to Web URLs on the Internet or on your corporate intranet. When you create Web bookmarks, you can insert the user's Secure Access device username in the URL path to provide single sign-on access to back-end Web applications. • Applet—Links the user to Java applets that you upload to the Secure Access device through the NSM by selecting Users > Resource Profiles > Web > Hosted Java Applets.

Table 19: User Role Web Rewriting Configuration Details (*continued*)

Option	Function	Your Action
URL	Specifies the URL to bookmark. NOTE: This box is displayed only when you select Standard from the Bookmark Type drop-down list.	Enter the URL.
Applet HTML	Specify an HTML page definition that includes references to your Java applets. NOTE: Enter a unique HTML page definition in this box. If you create two bookmarks with the same HTML code, the Secure Access device deletes one of the bookmarks in the end-user view. You can still see both bookmarks, however, in the administrator console. NOTE: The Applet HTML and Multi-Valued User Attributes fields are displayed only when you select Applet from the Bookmark Type drop-down list.	Enter the unique HTML page definition.
Multi-Valued User Attributes	Allows you to specify multiple attributes if your HTML code contains attributes that may expand to multiple values (such as userAttr.hostname or userAttr.ports), .	Enter multiple attributes.
Web > Options tab		
User can type URLs in IVE browse bar	Enables users to enter URLs on the welcome page.	Select the User can type URLs in Secure Access device browse bar check box to enable this feature.
Users can add bookmarks	Enables users to create personal Web bookmarks on the Secure Access device welcome page.	Select the User can add bookmarks check box to enable this feature.

Table 19: User Role Web Rewriting Configuration Details (*continued*)

Option	Function	Your Action
Mask hostnames while browsing	<p>Conceals the target resources in the URLs to which users browse.</p> <p>Users can mask IP addresses and hostnames in the user's:</p> <ul style="list-style-type: none"> • Web browser address bar (when the user navigates to a page.) • Web browser status bar (when the user hovers over a hyperlink.) • HTML source files (when the user chooses to view source.) 	<p>Select the Mask hostnames while browsing check box to enable this feature.</p>
Allow Java applets	<p>Enables users to: and allows user to</p> <ul style="list-style-type: none"> • Browse to web pages containing client-side Java applets. • Run applications that are implemented as client-side Java applets. • Run application such as the Virtual Network Computing (VNC) Java client, Citrix NFuse Java client, WRQ Reflection Web client, and Lotus WebMail. 	<p>Select the Allow Java applets check box to enable this feature.</p>
Allow Flash content	<p>Enables the Secure Access device to intermediate flash content through its Content Intermediation Engine.</p>	<p>Select the Allow Flash content check box to enable this feature.</p> <p>NOTE: Secure Access device provides limited support for ActionScript 2.0 Flash Remoting, and does not support XML Socket connections.</p>
Persistent cookies	<p>Enables users to customize their browsing experiences through persistent cookies.</p>	<p>Select the Persistent cookies to enable this feature.</p> <p>By default, the Secure Access device flushes Web cookies that are stored during a user session. A user can delete cookies through the Advanced Preferences if you enable this option.</p>

Table 19: User Role Web Rewriting Configuration Details (*continued*)

Option	Function	Your Action
Unrewritten pages open in new window	Allows configuration of Secure Access device to open content in a new browser window when a user accesses an unrewritten Web page.	Select the Unrewritten pages open in new window check box to enable this feature.
Allow browsing untrusted SSL websites	Enables users to access untrusted Web sites through the Secure Access device.	<p>Select the Allow browsing untrusted SSL Web sites check box to enable this feature.</p> <p>NOTE: If a Web page has internal references to files within a SCRIPT tag and these files are hosted on different HTTPS servers that have SSL certificates not trusted by the Secure Access device, the Web page does not render correctly. In these cases, the Warn users about the certificate problems option must be disabled.</p>
Warn users about the certificate problems	Notifies the user with a warning message at the time of first access on an untrusted web site.	<p>Select the Warn users about the certificate problems check box to enable this feature.</p> <p>NOTE: If you select this option and the user accesses non-HTML content (such as images, js, and css) served from an SSL server that differs from the HTML page, the page containing the links may not display correctly. You can avoid this problem either by clearing this option or by uploading a valid production SSL certificate on the servers that serve the non- HTML content.</p>
Allow users to bypass warnings on a server-by-server basis	Allows users to suppress all further warnings for an untrusted Web site. The user never sees a warning for this site, provided the user accesses it from the current Secure Access device or cluster.	<p>Select Allow users to bypass warnings on a server-by-server basis to enable this feature.</p> <p>NOTE: If you allow users to access untrusted Web sites without seeing a warning, the Secure Access device still logs a message to the user access log whenever a user navigates to an untrusted site. Also note that if a user chooses to suppress warnings, he can clear the persistent settings of the untrusted Web sites.</p>

Table 19: User Role Web Rewriting Configuration Details (*continued*)

Option	Function	Your Action
Rewrite file:// URLs	Allows the configuration of a Secure Access device to rewrite file:// URLs so that they are routed through the Secure Access device's file browsing CGI.	Select the Rewrite file:// URLs check box to enable this feature.
Rewrite links in PDF files	Allows the configuration of a Secure Access device to rewrite hyperlinks in PDFs.	Select the Rewrite links in PDF files check box to enable this feature.
HTTP Connection Timeout	Allows users to accept the default value or set the duration to tell the Secure Access device how long to wait for a response from an HTTP server before timing out and closing the connection.	Select a timeout value from 30 to 1800 seconds.

Related Documentation

- [Configuring Telnet/SSH on a Secure Access Device User Role \(NSM Procedure\) on page 89](#)
- [Configuring File Rewriting Resource Profiles \(NSM Procedure\) on page 120](#)
- [Configuring Web Rewriting Resource Policies \(NSM Procedure\) on page 151](#)

Configuring Telnet/SSH on a Secure Access Device User Role (NSM Procedure)

The Telnet/SSH option enables users to connect to internal server hosts in the clear using Telnet protocols or to communicate over an encrypted Secure Shell (SSH) session through a Web-based terminal session emulation.

To configure telnet/SSH on a user role:

1. In the navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure a telnet/SSH.
2. Click the **Configuration** tab. Select **Users > User Roles**.
3. Click the **New** button. The New Dialog box appears.
4. Add or modify settings on the access options as specified in [Table 20 on page 90](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 20: User Role Telnet/SSH Configuration Details

Option	Function	Your Action
Telnet/SSH > Telnet Bookmarks tab		
Name	Specifies the name for the Terminal Sessions page bookmark.	Enter the name for the bookmark.
Description	Specifies the bookmark description for the Terminal Sessions page bookmark.	Enter the description.
Host	Specifies the name or IP address of the remote host for this session.	Enter the name or IP address.
Session Type	Specifies the session type.	Select telnet or SSH from the drop-down list.
Port	Specifies the port if different from the prepopulated port assignment.	Enter the port.
Username	Specifies the username or other Secure Access device-appropriate, session variable for Telnet bookmark.	Enter a username or other Secure Access device-appropriate, session variable.
Font Size	Specifies the font size for the Telnet bookmark.	Select the font size.
Screen Size	Specifies the screen size for the telnet bookmark.	Select one of the options from drop-down list.
Screen Buffer	Specifies the screen buffer size for the Telnet bookmark.	Select the screen buffer size.
Telnet/SSH > Options tab		
User can add sessions	<p>Allows users to define their own session bookmarks and to allow users to browse to a terminal session using the following syntax:</p> <ul style="list-style-type: none"> telnet:// ssh:// /dana/term/newlaunchterm.cgi <p>The Add Terminal Session button appears on the Terminal Sessions page the next time a user refreshes the Secure Access device welcome page.</p>	Select the User can add sessions check box to enable this feature.

- Related Documentation**
- [Configuring Access Options using Remote Access Mechanisms Overview on page 65](#)
 - [Configuring a File Rewriting Resource Policy \(NSM Procedure\) on page 137](#)

CHAPTER 9

Configuring Secure Access Resource Profiles

- [Configuring a JSAM Resource Profile \(NSM Procedure\) on page 93](#)
- [Configuring a Citrix Terminal Services \(Custom ICA\) Resource Profile \(NSM Procedure\) on page 95](#)
- [Configuring a Citrix Terminal Services \(Default ICA\) Resource Profile \(NSM Procedure\) on page 99](#)
- [Configuring a Citrix Listed Application Resource Profile \(NSM Procedure\) on page 104](#)
- [Configuring Citrix Web Applications Resource Profile \(NSM Procedure\) on page 110](#)
- [Configuring Custom Web Applications Resource Profile \(NSM Procedure\) on page 112](#)
- [Configuring File Rewriting Resource Profiles \(NSM Procedure\) on page 120](#)
- [Configuring Windows Terminal Services \(NSM Procedure\) on page 124](#)
- [Configuring a Telnet/SSH Resource Profile \(NSM Procedure\) on page 129](#)
- [Configuring WSAM Resource Profile \(NSM Procedure\) on page 131](#)
- [Configuring Bookmarks for Virtual Desktop Resource Profiles \(NSM Procedure\) on page 134](#)

Configuring a JSAM Resource Profile (NSM Procedure)

A JSAM resource profile configures JSAM to secure traffic to a client/server application. When you create a JSAM application resource profile, the JSAM client tunnels network traffic generated by the specified client applications to servers in your internal network.

To create a JSAM application resource profile:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure JSAM application resource profile.
2. Click the **Configuration** tab, and select **Users > Resource Profiles > SAM > Client Applications**. The corresponding workspace appears.
3. Click the **New** button and the New dialog box appears.

4. Add or modify settings as specified in [Table 21 on page 94](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 21: Configuring JSAM Resource Profile details

Option	Function	Your Action
Settings tab		
Name	Specifies a name for the resource profile.	Enter the name.
Description	Describes the resource profile.	Enter the description.
Type	Allows you to select either JSAM or WSAM to configure resource profile.	Select JSAM option to configure JSAM resource profile.
Settings tab > JSAM > Custom		
Server Hostname or IP	Specifies the hostname or IP address of the remote server.	Enter the hostname or IP address.
Server Port	Specifies the port on which the remote server listens for client connections.	Enter the port.
Localhost IP	Specifies the IP address of the localhost.	Enter the IP address.
Client Port	Specifies the port on which JSAM should listen for client application connections.	Enter the port.
Create an access control policy allowing SAM access to these servers	Allows access to the list of servers specified in the Server Port column	Select the Create an access control policy allowing SAM access to these servers check box to enable this feature.
Allow JSAM to dynamically select an available port if the specified client port is in use	Allows JSAM to select an available port when the client port you specify is taken. The client application must allow you to specify the port number for the connection to use this option.	Select the Allow JSAM to dynamically select an available port if the specified client port is in use check box to enable this option.
Settings > Lotus Notes > Autopolicy: SAM Access Control > Rules tab		
Name	Specifies the name of the policy.	Enter the name.
Resources	Specifies the application server to which this policy applies.	Enter the application resource name.
Action	Allows or denies user access to the resources.	Select either Allow or Deny from the Action drop-down list.

Table 21: Configuring JSAM Resource Profile details (*continued*)

Option	Function	Your Action
Settings > Microsoft Outlook/Exchange		
New Application Servers	Specifies the hostname for the MS Exchange server.	Enter the hostname
Create an access control policy allowing SAM access to these servers	Enables user to access the server specified in the previous step, application servers (enabled by default).	Select the Create an access control policy allowing SAM access to these servers check box to enable this option.
Settings tab > NetBIOS File Browsing		
New Application Servers	Specifies the fully qualified hostname for your application servers.	Enter the hostname.
Create an access control policy allowing SAM access to these servers	Allows user access the server specified in the previous step, application servers (enabled by default).	Select the Create an access control policy allowing SAM access to these servers check box to enable this option.
Settings > Roles tab		
Roles Selections	Specifies the roles to which the resource profile applies.	Select the role and, then click Add to move the role from the Non-members to the Members list.

Related Documentation

- [Configuring a Citrix Terminal Services \(Custom ICA\) Resource Profile \(NSM Procedure\) on page 95](#)
- [Configuring a Citrix Terminal Services \(Default ICA\) Resource Profile \(NSM Procedure\) on page 99](#)

Configuring a Citrix Terminal Services (Custom ICA) Resource Profile (NSM Procedure)

Use this type of resource profile to enable a terminal session on a Citrix Metaframe server using settings that you specify in a customized ICA file.

To configure a Citrix resource profile that uses a custom ICA file:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure a Citrix terminal services resource profile that uses custom ICA settings.
2. Click the **Configuration** tab, and select **Users > Resource Profiles > Terminal Services**. The corresponding workspace appears.
3. Click the **New** button and the New dialog box appears.
4. Add or modify settings as specified in [Table 22 on page 96](#).
5. Click one:

- **OK**—Saves the changes.
- **Cancel**—Cancels the modifications.

Table 22: Citrix Terminal Services (Custom ICA) Resource Profile Configuration Details

Option	Function	Your Action
Settings tab		
Name	Specifies a unique name for the resource profile.	Enter the name.
Description	Describes the resource profile.	Enter the description.
Java Support Options	Allows you to enable or disable Java applet support.	<p>Select one of the following options from the Java Support Options drop-down list:</p> <ul style="list-style-type: none"> • Disable Java Support—Disables Java support for a Secure Access device to intermediate traffic. • Use Java applet as a fallback mechanism—Allows a Secure Access device to fall back to the applets when other terminal services clients are not available on the user's system. • Always use Java applet—Allows a Secure Access device to store terminal services Java clients directly on the Secure Access device without employing a separate Web server to host them. You can then associate these Java applets with the resource profile and specify that the Secure Access device always use them to intermediate traffic.
Applet to use	Specifies the Java applet that you want to associate with the resource profile.	Select a Java applet from the Applet to use drop-down list.

Table 22: Citrix Terminal Services (Custom ICA) Resource Profile Configuration Details *(continued)*

Option	Function	Your Action
Applet HTML	Specifies the HTML page definition that includes references to your Java applets.	Enter the HTML page definition. NOTE: The maximum size of the HTML that can be specified is 25KB.
Type	Allows you to specify the terminal service.	Select Citrix using Custom ICA option to configure a citrix resource profile that uses a custom ICA file.
Citrix using Custom ICA > Settings tab		
Custom ICA File	Specifies the ICA file that contains the session parameters that you want use.	Click the Browse button to select an ICA file.
Custom ICA Filename	Specifies the unique name for the custom ICA file.	Enter the name.
Citrix using Custom ICA > Autopolicy: Terminal Services Access control > Rules tab		
Name	Specifies the name of a policy that allows or denies users access to the resource profile.	Enter a name.
Action	Enables you to allow or deny user access to resource.	Select either Allow or Deny from the Action drop-down list.
Resources	Specifies the metaframe servers to which you want to enable access.	Enter the metaframe server.
Citrix using Custom ICA > Bookmarks		
Name	Specifies the name of the session bookmark.	Enter the name.
Description	Describes the resource profile.	Enter a description.
Username	Specifies the username that the Secure Access device should pass to the terminal server.	Enter the username.

Table 22: Citrix Terminal Services (Custom ICA) Resource Profile Configuration Details *(continued)*

Option	Function	Your Action
Password Type	Specifies the static password or variable password. You can also use the password stored in the Secure Access device's primary or secondary authentication server. Or you can use the domain credentials to pass the user's cached domain credentials to the Windows Terminal Services server.	Select either Variable Password or Password from the Password Type drop-down list.
Variable Password	Specifies the variable password.	Enter the <password> variable. Or use the following syntax to submit the password for the secondary authentication server: <Password@Secondary ServerName> or <Password[2]> .
Explicit Password	Specifies the explicit password.	Enter the explicit password.
Auto-launch	Allows you to automatically launch this terminal services session bookmark when users sign into the Secure Access device.	Select the Auto-launch check box to enable this feature.
Applies to roles	Specifies the roles to which you want to display the session bookmarks.	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • All Terminal Service Profile roles—Displays the session bookmark to all of the roles associated with the resource profile. • Subset of Terminal Service Profile roles—Displays the session bookmark to a subset of the roles associated with the resource profile. Then select roles from the ALL Selected Roles list and click Add to move them to the Subset of selected roles list.

Settings > Role Selections tab

Table 22: Citrix Terminal Services (Custom ICA) Resource Profile Configuration Details *(continued)*

Option	Function	Your Action
Roles Selections	Specifies the roles to which the resource profile applies. NOTE: The Role Selections tab is enabled only when you select the Subset of Terminal Service Profile roles check box from the Applies to roles drop down list.	Select the role and, click Add .

Related Documentation

- [Configuring a Citrix Terminal Services \(Default ICA\) Resource Profile \(NSM Procedure\) on page 99](#)
- [Configuring a Citrix Listed Application Resource Profile \(NSM Procedure\) on page 104](#)
- [Configuring a JSAM Resource Profile \(NSM Procedure\) on page 93](#)

Configuring a Citrix Terminal Services (Default ICA) Resource Profile (NSM Procedure)

Use this type of resource profile to enable a terminal session on a Citrix Metaframe server using settings that you specify in a default Citrix file (ICA).

To configure a Citrix terminal services resource profile that uses default ICA settings:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure a Citrix terminal services resource profile that uses default ICA settings.
2. Click the **Configuration** tab, and select **Users > Resource Profiles > Terminal Services**. The corresponding workspace appears.
3. Click the **New** button and the New dialog box appears.
4. Add or modify settings as specified in [Table 23 on page 99](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 23: Citrix Terminal Services (Default ICA) Configuration Details

Option	Function	Your Action
Settings tab		
Name	Specifies a unique name for the resource profile.	Enter the name.
Description	Describes the resource profile.	Enter the description.

Table 23: Citrix Terminal Services (Default ICA) Configuration Details (*continued*)

Option	Function	Your Action
Java Support Options	Allows you to enable or disable Java applet support.	<p>Select one of the following options from the Java Support Options drop-down list:</p> <ul style="list-style-type: none"> • Disable Java Support—Disables Java support for a Secure Access device to intermediate traffic. • Use Java applet as a fallback mechanism—Allows a Secure Access device to fall back to the applets when other terminal services clients are not available on the user's system. • Always use Java applet—Allows a Secure Access device to store terminal services Java clients directly on the Secure Access device without employing a separate Web server to host them. You can then associate these Java applets with the resource profile and specify that the Secure Access device always use them to intermediate traffic.
Applet to use	Specifies the Java applet that you want to associate with the resource profile.	Select a Java applet from the Applet to use drop-down list.
Applet HTML	Specifies the HTML page definition that includes references to your Java applets.	<p>Enter the HTML page definition.</p> <p>NOTE: The maximum size of the HTML that can be specified is 25 KB.</p>
Type	Allows you to specify the type of terminal service.	Select Citrix using default ICA option to configure a citrix terminal services resource profile that uses default ICA.

Citrix using default ICA > Settings tab

Table 23: Citrix Terminal Services (Default ICA) Configuration Details (*continued*)

Option	Function	Your Action
Host	Specifies the server and port to which this resource profile should connect.	Enter a hostname or IP address.
Server Port	Specifies the port on which the terminal server listens.	Enter the port. NOTE: By default, the Secure Access device populates this field with port number 1494 for Citrix.
Create an access control policy	Allows you to access the server specified in the Server Port box (enabled by default).	Select the Create an access control policy check box to enable this feature.
Citrix using default ICA > Bookmarks tab > General tab		
Name	Specifies the name of the session bookmark.	Enter the name.
Description	Describes the session bookmark.	Enter a description.
Host	Specifies the existing host of the resource profile that connects to a Citrix terminal server on the Secure Access device.	The Secure Access device automatically populates the Host box using settings from the selected resource profile
Server Port	Specifies the existing server port of the resource profile that connects to a Windows terminal server on the Secure Access device.	The Secure Access device automatically populates the Server Port box using settings from the selected resource profile.
Screen Size	Specifies the screen size of the terminal services window on the user's workstation.	Select the screen size from the drop-down list. NOTE: By default, the Secure Access device sets the window size to full screen.
Color Depth	Allows you to change the color-depth of the terminal session data.	Select the color depth from the drop-down list. NOTE: By default, the Secure Access device sets the color depth to 8-bit.
Username	Specifies the username that the Secure Access device should pass to the terminal server.	Enter the username.

Table 23: Citrix Terminal Services (Default ICA) Configuration Details (*continued*)

Option	Function	Your Action
Password Type	Allows you to select static either a password or a variable password that the Secure Access device should pass to the terminal server.	Select one of the following options from the Password Type drop-down list: <ul style="list-style-type: none"> • Variable Password—Uses the password stored in the Secure Access device's primary or secondary authentication server. • Password—Allows you to specify a password.
Variable Password	Specifies the variable password.	Enter the <password> variable. Or use the following syntax to submit the password for the secondary authentication server: <Password@SecondaryServerName> or <Password[2]> .
Explicit Password	Specifies the explicit password.	Enter the explicit password.
Path to application	Specifies where the application's executable file resides on the terminal server.	Enter the path. For example, you might enter the following directory for the Microsoft Word application: C:\Program Files\Microsoft Office\Office10\WinWord.exe
Working directory	Specifies where the terminal server should place working files for the application.	Enter the path. For example, you might specify that Microsoft Word should save files to the following directory by default: C:\Documents and Settings\username\My Documents
Auto-launch	Allows you to automatically launch this Terminal Service session bookmark when users sign into the Secure Access device.	Select the Auto-launch check box to enable this feature.
Connect drives	Allows you to connect the user's local drive to the terminal server, enabling the user to copy information from the terminal server to his local client directories.	Select the Connect drives check box to enable this feature.

Table 23: Citrix Terminal Services (Default ICA) Configuration Details (*continued*)

Option	Function	Your Action
Connect printers	Allows you to connect the user's local printers to the terminal server, enabling the user to print information from the terminal server to his local printer.	Select the Connect printers check box to enable this feature.
Connect COM Ports	Allows you to connect the user's COM ports to the terminal server, allowing communication between the terminal server and the devices on his serial ports.	Select the Connect COM Ports check box to enable this feature.
Session Reliability and Auto-client reconnect	Allows ICA sessions active and on the user's screen when network connectivity is interrupted. Users continue to see the application they are using until the network connectivity resumes or the session reliability time-out has expired (the time-out value is defined by the Citrix product).	Select the Session Reliability and Auto-client reconnect check box to enable this feature.
Port to be enabled	Specifies the port to use.	Select the Port to be enabled check box to enable this feature.
Applies to roles	Specifies the roles to which you want to display the session bookmarks.	<p>Select one of the following options from the Applies to roles drop-down list:</p> <ul style="list-style-type: none"> • All Terminal Service Profile roles—Displays the session bookmark to all of the roles associated with the resource profile. • Subset of Terminal Service Profile roles—Displays the session bookmark to a subset of the roles associated with the resource profile. Then select roles from the ALL Selected Roles list and click Add to move them to the Subset of selected roles list.
Settings > Role Selections tab		

Table 23: Citrix Terminal Services (Default ICA) Configuration Details (*continued*)

Option	Function	Your Action
Roles Selections	Specifies the roles to which the resource profile applies. NOTE: The Role Selections tab is enabled only when you select the Subset of Terminal Service Profile roles check box from the Applies to roles drop-down list.	Select the role, and then click Add .

Related Documentation

- [Configuring a Citrix Listed Application Resource Profile \(NSM Procedure\) on page 104](#)
- [Configuring Custom Web Applications Resource Profile \(NSM Procedure\) on page 112](#)
- [Configuring a Citrix Terminal Services \(Custom ICA\) Resource Profile \(NSM Procedure\) on page 95](#)

Configuring a Citrix Listed Application Resource Profile (NSM Procedure)

Citrix created *published applications* to satisfy the need for security. It is dangerous to allow any executable to be run on the server. With published applications, only applications that are allowed to be run are published.

With the Secure Access device, these published applications are displayed on the Secure Access device index page as terminal services bookmarks.

To configure a Citrix listed application resource profile:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure a Citrix listed application resource profile.
2. Click the **Configuration** tab, and select **Users > Resource Profiles > Terminal Services**. The corresponding workspace appears.
3. Click the **New** button and the New dialog box appears.
4. Add or modify settings as specified in [Table 24 on page 104](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 24: Citrix Listed Application Resource Profile Configuration Details

Option	Function	Your Action
Settings tab		
Name	Specifies a unique name for the resource profile.	Enter the name.

Table 24: Citrix Listed Application Resource Profile Configuration Details (*continued*)

Option	Function	Your Action
Description	Describes the resource profile.	Enter a description.
Java Support Options	Allows you to enable or disable Java applet support.	<p>Select one of the following options from the Java Support Options drop-down list:</p> <ul style="list-style-type: none"> • Disable Java Support—Disables a Java support for Secure Access device to intermediate traffic. • Use Java applet as a fallback mechanism—Allows a Secure Access device to fall back to the applets when other terminal services clients are not available on the user's system. • Always use Java applet—Allows a Secure Access device to store terminal services Java clients directly on the Secure Access device without employing a separate Web server to host them. You can then associate these Java applets with the resource profile and specify that the Secure Access device always use them to intermediate traffic.
Applet to use	Specifies the Java applet that you want to associate with the resource profile.	Select a Java applet from the Applet to use drop-down list.
Applet HTML	Specifies the HTML page definition that includes references to your Java applets.	<p>Enter the HTML page definition.</p> <p>NOTE: The maximum size of the HTML that can be specified is 25 KB.</p>
Type	Specifies the terminal service.	Select Citrix Listed Applications option to enable this feature.
Citrix Listed Applications > Settings tab		

Table 24: Citrix Listed Application Resource Profile Configuration Details (*continued*)

Option	Function	Your Action
Citrix XML Service IP and Port	Specifies the IP address and port of the Citrix MetaFrame server where the XML service is running.	Enter the IP address and port of the Citrix MetaFrame server. NOTE: <ul style="list-style-type: none"> You do not need to enter the port number if you are using the default value. The default port is 80 (if SSL is selected, the default port is 443). You can enter more than one server. If the connection fails on one server, the next server in the list is used.
Use SSL for connecting to Citrix XML Service	Sends the password through SSL instead of cleartext.	Select the Use SSL for connecting to Citrix XML Service check box to enable this feature.
XML Username	Specifies the username for connecting to the Citrix Metaframe server where the XML service is running.	Enter the username for connecting to the Citrix Metaframe server.
XML Password Type	Specifies static password or variable password.	Select either Variable Password or Password from the drop-down list.
Variable Password	Specifies the variable credentials. NOTE: This field is enabled only when you select Variable Password from the XML Password Type drop-down list.	Enter the variable credential such as <USERNAME> and<PASSWORD>.
XML Password	Specifies the XML password. NOTE: This field is enabled only when you select XML Password from the XML Password Type drop-down list.	Enter the XML password.
XML Domain	Specifies the domain name for connecting to the Citrix Metaframe server where the XML service is running.	Enter the domain name.

Citrix Listed Applications > Autopolicy: Terminal Services Access Control > Rules tab

Table 24: Citrix Listed Application Resource Profile Configuration Details (*continued*)

Option	Function	Your Action
Name	Specifies the name of a policy that allows or denies users access to the resource.	Enter a name.
Action	Allows or denies user access to resource.	Select either Allow or Deny from the Action drop-down list.
Resource	Specifies the resource name for which you want to enable access.	Enter the resource name.
Citrix Listed Applications > Bookmarks tab > General tab		
Name	Specifies the name of the session bookmark of the resource profile.	Enter the name.
Description	Describes the session bookmark of the resource profile.	Enter a description.
Applications	Specifies the applications you want available to the end user.	<p>Select one of the following options from the Applications drop-down list.</p> <ul style="list-style-type: none"> • ALL applications—Allows all executables on the server to be available to the end user. • Subset of selected applications—Allows you to select executables that you want available to the end user. <p>NOTE: This option is disabled when you enter variable credentials, such as <USERNAME> and <PASSWORD> while defining the resource profile.</p>
Selected Applications	Specifies the executables to run.	Enter the executables.
Username	Specifies the username that the Secure Access device should pass to the terminal server. You can enter a static username or a variable.	Enter the username.

Table 24: Citrix Listed Application Resource Profile Configuration Details (continued)

Option	Function	Your Action
Password Type	Specifies a static or variable password. If you select a variable password, then you can use the password stored in the Secure Access device's primary or secondary authentication server, or you can use the domain credentials to pass the user's cached domain credentials to the Windows Terminal server.	<p>Select one of the following options from the Password Type drop-down list:</p> <ul style="list-style-type: none"> • Variable Password—Uses the password stored in the Secure Access device's primary or secondary authentication server. • Explicit Password—Allows you to specify a static password. • Use domain credentials—Passes the user's cached domain credentials to the Citrix Metaframe server (also called pass-through authentication). When you select this option, the Secure Access device uses the Citrix Program Neighborhood client to intermediate the Citrix terminal session.
Variable Password	Specifies the variable password.	<p>Enter the <password> variable. Or use the following syntax to submit the password for the secondary authentication server:</p> <p><Password@SecondaryServerName> or <Password[2]>.</p>
Explicit Password	Specifies the explicit password.	Enter the explicit password.
Session Reliability and Auto-client reconnect	Keeps sessions active and on the user's screen when network connectivity is interrupted.	Select the Session Reliability and Auto-client reconnect check box to enable this feature.
Screen Size	Specifies the size of the terminal services window on the user's workstation.	<p>Select screen size from the drop-down list.</p> <p>NOTE: By default, the Secure Access device sets the window size to full screen.</p>
Color Depth	Changes the color-depth of the terminal session data.	Select color depth the drop-down list.

Table 24: Citrix Listed Application Resource Profile Configuration Details (*continued*)

Option	Function	Your Action
Connect drives	Connects the user's local drive to the terminal server, enabling the user to copy information from the terminal server to his local client directories.	Select the Connect drives check box to enable this feature.
Connect printers	Connects the user's local printers to the terminal server, enabling the user to print information from the terminal server to his local printer.	Select the Connect printers check box to enable this feature.
Connect COM Ports	Connects the user's COM ports to the terminal server, allowing communication between the terminal server and the devices on his serial ports.	Select the Connect COM Ports check box to enable this feature.
Applies to roles	Specifies the roles to which you want to display the session bookmarks.	<p>Select one of the following options from the drop-down list`:</p> <ul style="list-style-type: none"> • All Terminal Service Profile roles—Displays the session bookmark to all of the roles associated with the resource profile. • Subset of Terminal Service Profile roles—Displays the session bookmark to a subset of the roles associated with the resource profile. Then select roles from the ALL Selected Roles list and click Add to move them to the Subset of selected roles list.
Settings > Role Selections tab		
Roles Selections	<p>Specifies roles to which the resource profile applies.</p> <p>NOTE: The Role Selections tab is enabled only when you select Subset of Terminal Service Profile roles option from the Applies to roles drop-down list.</p>	Select the role, and click Add .

Related Documentation

- [Configuring Custom Web Applications Resource Profile \(NSM Procedure\) on page 112](#)
- [Configuring File Rewriting Resource Profiles \(NSM Procedure\) on page 120](#)

- [Configuring a Citrix Terminal Services \(Default ICA\) Resource Profile \(NSM Procedure\)](#) on page 99

Configuring Citrix Web Applications Resource Profile (NSM Procedure)

The Citrix Web template enables you to easily configure Citrix access using the Juniper Networks Citrix Terminal Services proxy, JSAM, or WSAM.

To configure a Citrix Web application resource profile:

1. In the NSM navigation tree, select **Device Manager** > **Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure a Citrix Web application resource profile.
2. Click the **Configuration** tab, and select **Users** > **Resource Profiles** > **Web**.
3. Click the **New** button and the New dialog box appears.
4. Select **Citrix Web Interface/JICA** from the Type list.
5. Enter a unique name and optionally a description for the Citrix resource profile.
6. Add or modify settings as specified in [Table 25 on page 110](#).
7. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 25: Citrix Web Application Configuration Details

Options	Your Action
Web Interface (NFuse) URL	<p>Enter the URL of the Web server that hosts your ICA files.</p> <p>Use the format: <i>[protocol://]host[:port][/path]</i>. For instance, enter the URL of an NFuse server, the Web interface for a Citrix Metaframe Presentation Server, or a Web server from which the device can download Citrix Java applets or Citrix cab files.</p>
Citrix implementation type	<p>Specify which type of Citrix implementation you are using in your environment by selecting one of the following options:</p> <ul style="list-style-type: none"> • Java ICA Client with Web Interface (NFuse)—Select this option if you have deployed the Citrix Web Interface for MPS (that is, NFuse) to deliver Java ICA clients. • Java ICA Client without Web Interface (NFuse)—Select this option if you have deployed a generic Web server to deliver Java ICA clients. • Non-Java ICA Client with Web Interface (NFuse)—Select this option if you have deployed the Citrix Web Interface for MPS (that is, NFuse) to use any of the different clients (Java, ActiveX, local). • Non-Java ICA Client without Web Interface (NFuse)—(Read only) If you have deployed a non-Java ICA client without the Citrix Web Interface for MPS (that is, NFuse), you cannot create a Citrix resource profile through this template. Instead, click the Client Application Profile link beneath this option.
Web Interface (NFuse) version	Select the required Citrix version from the drop-down list.

Table 25: Citrix Web Application Configuration Details (*continued*)

Options	Your Action
MetaFrame servers	<p>Specify the Metaframe presentation servers to which you want to control access.</p> <p>Click Add. When specifying servers, you can enter wildcards or IP ranges.</p> <p>The device uses the values that you enter to automatically create a resource policy that enables access to the necessary resources. They include:</p> <ul style="list-style-type: none"> • If you select either Java ICA Client with or without Web Interface, the device creates a Java ACL resource policy that enables Java applets to connect to the specified Metaframe servers. • If you select Non-Java ICA Client with Web Interface, and then you select ICA client connects over WSAM or JSAM, the device creates a corresponding SAM resource policy that enables users to access the specified Metaframe servers. • If you select Non-Java ICA Client with Web Interface, and then you select ICA client connects over CTS, the device creates corresponding Terminal Services and Java resource policies that enable users to access the specified Metaframe servers.
Sign applets with uploaded code-signing certificate(s)	<p>Enable this check box to re-sign the specified resources using the certificate uploaded after selecting System > Configuration > Certificates > Code-signing Certificates page.</p> <p>NOTE: This option is for Java ICA clients only. Enable this option only if you have deployed Citrix using a Java ICA client.</p> <p>When you select this option, the device uses all of the “allow” values that you enter in the resource profile’s Web access control autopolicy to automatically create a corresponding code-signing resource policy. Within this policy, the device uses the specified Web resources to create a list of trusted servers.</p>
Configure access to local resources	<p>Enable this check box to allow users to access local resources such as printers and drives through their Citrix Web interface sessions. Select one of the following options after enabling this option:</p> <ul style="list-style-type: none"> • Select Connect printers if you want to enable the user to print information from the terminal server to the local printer. • Select Connect drives if you want to enable the user to copy information from the terminal server to the local client directories. • Select Connect COM Ports if you want to enable communication between the terminal server and devices on the user’s serial ports.
Autopolicy: Web Access Control	<p>Enable this check box to create a policy that allows or denies users access to the resource specified in the Web Interface (NFuse) URL box. By default, the device automatically creates a policy for you that enables access to the resource and all of its subdirectories.</p>
Roles	<p>Select the roles to which the Citrix resource profile applies.</p>



NOTE: If you selected one of the Web interface options from the [Table 25 on page 110](#), then update the SSO policy created by the Citrix template. Select the **Autopolicy: Single Sign-on** check box. (Single sign-on autopolicies configure the device to automatically pass device data such as usernames and passwords to the Citrix application. The device automatically adds the most commonly used values to the single sign-on autopolicy based on the Citrix implementation you choose).

The selected roles inherit the autopolicies and bookmarks created by the Citrix resource profile. If it is not already enabled, the device also automatically enables the Web option in the Users > User Roles > Select_Role > General > Overview page of the admin console and the Allow Java Applets option in the Users > User Roles > Select_Role > Web > Options page of the NSM UI for all of the roles you select.

In the Bookmarks tab, you can optionally modify the default bookmark created by the device and/or create new ones. (By default, the device creates a bookmark to the Web interface (NFuse) URL defined in the Web Interface (NFuse) URL field and displays it to all users assigned to the role specified in the Roles tab).

Related Documentation

- [Configuring a Citrix Listed Application Resource Profile \(NSM Procedure\) on page 104](#)
- [Configuring Custom Web Applications Resource Profile \(NSM Procedure\) on page 112](#)
- [Configuring a Citrix Terminal Services \(Default ICA\) Resource Profile \(NSM Procedure\) on page 99](#)

Configuring Custom Web Applications Resource Profile (NSM Procedure)

A custom Web application resource profile is a resource profile that controls access to a Web application, Web server, or HTML page.

To configure a custom Web application resource profile:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure the Web application resource profile.
2. Click the **Configuration** tab, and select **Users > Resource Profiles > Web** to create a custom Web resource profile.
4. Click the **New** button, the New dialog box appears.
5. Add or modify settings as specified in [Table 26 on page 113](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 26: Configuring Custom Web Applications Resource Profile Details

Option	Function	Your Action
Settings tab		
Name	Specifies a unique name for the resource profile.	Enter the name.
Description	Specifies a description for the resource profile.	Enter the description.
Type	Specifies the type of resource profile.	Select Custom from the Type drop-down list.
Base URL		
Base URL	Specifies the URL of the Web application or page for which you want to control access.	Enter the URL using the format: [protocol://]host[:port][/path]
Autopolicy: Web Access Control > Rules tab		
Name	Specifies the name for the policy that allows or denies users access to the resource specified in the Base URL box.	Enter the name.
Action	Allows or denies user access to the resource.	Select Allow or Deny from the Action drop-down list.
Resources	Specifies the resource for which this policy applies.	Enter the resource name.
Autopolicy: Basic Authentication, NTLM or Kerberos Single Sign-On		
Resource	Specifies the resource for which this policy applies.	Specify the resource.
Authentication Type	Specifies the authentication type.	Select the authentication type.
Autopolicy: From POST Single Sign-On		
Resource	Specifies the application's sign-in page.	Enter the path, such as: http://my.domain.com/public/login.cgi . NOTE: Do not enter wildcard characters in this box.
POST URL	Specifies the absolute URL where the application posts the user's credentials.	Enter the URL, such as: http://yourcompany.com/login.cgi .

Table 26: Configuring Custom Web Applications Resource Profile Details (*continued*)

Option	Function	Your Action
Deny direct login for this resource	Prevents users from manually entering their credentials in a sign-in page. (Users may see a sign-in page if the form POST fails.)	Select the Deny direct login for this resource check box to enable this option.
Allow multiple POSTs to this resource	Allows the Secure Access device to send POST and cookie values to the resource multiple times if required. If you do not select this option, the Secure Access device does not attempt single sign-on when a user requests the same resource more than once during the same session.	Select the Deny direct login for this resource check box to enable this option.
POST Variables		
Label	Specifies the label that appears on a user's preferences page in the Secure Access device. This field is required if you either enable or require users to modify data to post to back-end applications.	Enter the label name.
Name	Identifies the data in the Value box.	Enter the name.
Value	Specifies a value to post to the form.	Enter the value. You can enter static data or a system variable.
User Modifiable?	Allows or denies user to change the information in the Value box.	Select any one of the following option: <ul style="list-style-type: none"> • Not Modifiable— User is not able to change the information in the Value box. • User Can Modify—User can specify data for a back-end application. • User Must Modify—User must enter additional data to access a back-end application.
Autopolicy: Cookies and Headers Single Sign-On		

Table 26: Configuring Custom Web Applications Resource Profile Details (*continued*)

Option	Function	Your Action
Resource	Specifies the resources to which this policy applies to post header data to the specified URL when a user makes a request to a resource.	Specify the resource.
Header name	Specifies the text for the Secure ccess device to send as header data.	Enter the name.
Header Value	Specifies the value for the specified header.	Enter the value.
Autopolicy: Caching		
Name	Specifies the policy name.	Enter a name.

Table 26: Configuring Custom Web Applications Resource Profile Details (*continued*)

Option	Function	Your Action
Action	Specifies the action to perform by the cache cleaner on the resource.	<p>Select one of the following option:</p> <ul style="list-style-type: none"> • Smart Caching (send headers appropriate for content and browser)—Allows the Secure Access device to send a cache-control:no-store header or a cache-control:no-cache header based on the user's Web browser and content type. • Don't Cache (send "Cache Control: No Store")—Delivers attachments to Internet Explorer without saving them to the disk. (The browser temporarily writes files to the disk, but immediately removes them once it has opened the file in the browser.) • Don't Cache (send "Pragma: No Cache")—Prevents the user's browser from caching files to the disk. • Unchanged (do not add/modify caching headers)—Secure Access device forwards the origin server's caching headers as is. • Remove Cache-Control: No-Cache/No-Store—Removes the Cache Control:No Cache and Pragma:no-cache headers.
Resource	Specifies the resources to which this policy applies.	Enter the resource name.
Autopolicy: Java Applet Access Control		
Name	Specifies the name of the policy.	Enter the policy name.
Server Resource	Specifies the server resources to which this policy applies.	Enter the path using the format: host:[ports] .

Table 26: Configuring Custom Web Applications Resource Profile Details (*continued*)

Option	Function	Your Action
Action	Allows or denies Java applets to connect to the servers	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • Allow Socket Access—Allows Java applets to connect to the servers (and optionally ports) in the resource list. • Deny Socket Access—Prevents Java applets from connecting to the servers (and optionally ports) in the resource list.
Sign Java applets with uploaded code-signing certificate(s)	Resigns the specified resources using the uploaded certificate.	Select the Sign Java applets with uploaded code-signing certificate(s) check box to enable this option.
Autopolicy: Rewriting Options > Passthrough Proxy tab		
Use virtual hostname	Specifies the hostname alias for the application server. When the Secure Access device receives a client request for the application server hostname alias, it forwards the request to the specified application server port in the Base URL box.	Enter the hostname.
Use IVE port	Specifies a unique Secure Access device port in the range 11,000-11,099.	Enter the port in the range 11,000-11,099.
Rewrite XML	Allows Secure Access device to rewrite URLs contained within XML content. If this option is disabled, the Secure Access device passes the XML content "as is" to the server.	Select the Rewrite XML tab check box to enable this option.
Rewrite external links	Allows Secure Access device to rewrite all the URLs presented to the proxy. If this option is disabled, the Secure Access device rewrites only those URLs where the hostname is configured as part of the passthrough proxy policy.	Select the Rewrite external links check box to enable this option.

Table 26: Configuring Custom Web Applications Resource Profile Details (*continued*)

Option	Function	Your Action
Block cookies from being sent to the browser	Allows Secure Access device to block cookies destined for the client's browser. The Secure Access device stores the cookies locally and sends them to applications whenever they are requested.	Select the Block cookies from being sent to the browser check box to enable this option.
Host-Header forwarding	Allows Secure Access device to pass the hostname as part of the host header instead of the actual host identifier.	Select Host-Header forwarding to enable this option.

Autopolicy: Rewriting Options > No rewriting (use JSAM) > JSAM Parameters

Server Hostname or IP	Specifies the DNS name of the application server or the server IP address.	Enter the DNS name of the application server or the server IP address.
Server Port	Specifies the port on which the remote server listens for client connections.	Enter the port.
Localhost IP	Specifies a static loopback address. If you do not provide a static IP loopback address, the Secure Access device assigns an IP loopback address dynamically.	Enter the IP address.
Client Port	Specifies the port on which JSAM should listen for client application connections.	Enter the port.
Launch JSAM	Automatically starts JSAM when the Secure Access device encounters the base URL.	Select the Launch JSAM check box to enable this option.

Autopolicy: Rewriting Options > No rewriting (use JSAM) > Allowed WSAM Servers

Network Destination	Specifies resources for which WSAM secures client/server traffic between the client and the Secure Access device. By default, the Secure Access device extracts the correct server from the Web access control policy. You may choose to use this server as-is, modify it, and/or add new servers to the list.	Enter the hostname (the wild cards '*' or '?' are accepted) or an IP/netmask pair. Specify multiple ports for a host as separate entries.
---------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------

Autopolicy: Rewriting Options > No rewriting tab

Table 26: Configuring Custom Web Applications Resource Profile Details (*continued*)

Option	Function	Your Action
No rewriting	Automatically creates a selective rewriting policy for the autopolicy's URL.	Select the No rewriting check box to enable this option.
Autopolicy: Web Compression		
Name	Specifies the policy name.	Enter the policy.
Action	Allows the Secure Access device to compress the supported content type for the specified resource.	Select one of the following options: <ul style="list-style-type: none"> • Compress—Secure Access device compresses the supported content types from the specified resource. • Do not compress—Secure Access device does not compress the supported content types from the specified resource.
Resource	Specifies the resources to which this policy applies.	Enter the resource name.
Settings tab > Type > Custom > Bookmarks > General		
Name	Specifies the name of the bookmark.	Enter the name.
Description	Describes the bookmark.	Enter the description.
URL	Adds a suffix to the URL if you want to create links to subsections of the domain defined in the primary resource profile.	Enter a suffix to the URL.
Open New Window	Allows the enable Secure Access device to automatically open the Web resource in a new browser window.	Select the Open New Window check box to enable this option.
Do Not Display Address Bar	Removes the address bar from the browser.	Select the Do Not Display Address Bar check box to enable this feature.

Table 26: Configuring Custom Web Applications Resource Profile Details (*continued*)

Option	Function	Your Action
Do Not Display Tool Bar	Removes the menu and toolbar from the browser. This feature removes all menus, browsing buttons, and bookmarks from the browser window so that the user browses only through the Secure Access device.	Select the Do Not Display Tool Bar check box to enable this feature.
Applies to roles	Specifies the roles to which you want to display the bookmark.	<p>Select any one of the following options:</p> <ul style="list-style-type: none"> • All Web Profile roles—Displays the bookmark to all of the roles associated with the resource profile. • Subset of Web Profile roles—Displays the bookmark to a subset of the roles associated with the resource profile. Then select roles from the ALL Selected Roles list and click Add to move them to the Subset of selected roles list.
Settings tab > Type > Custom > Bookmarks > Role Selections		
Role Selections	Specifies the roles to which the resource profile applies.	Select the role, and click Add .

Related Documentation

- [Configuring File Rewriting Resource Profiles \(NSM Procedure\) on page 120](#)
- [Configuring Windows Terminal Services \(NSM Procedure\) on page 124](#)
- [Configuring a Citrix Listed Application Resource Profile \(NSM Procedure\) on page 104](#)

Configuring File Rewriting Resource Profiles (NSM Procedure)

A file resource profile controls access to resources on Windows server shares.

To configure a file rewriting resource profile:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure user roles.
2. Click the **Configuration** tab, and select **Users > Resource Profiles > Windows File Browsing** to create a resource profile to control access to Windows server shares.
3. Add or modify settings as specified in [Table 27 on page 121](#).

4. Click the **New** button, the New dialog box appears.
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 27: Configuring File Rewriting Resource Profiles Details

Option	Function	Your Action
Settings tab		
Name	Specifies the name of the resource profile.	Enter the name.
Description	Describes the resource profile.	Enter the description.
Server/share	Specifies the resource to which you want to control access.	Enter the server name or IP address, share name, and optionally the path that you want to control access. When entering the resource, use the format: \\server[\share[path]].
Autopolicy:Windows File Access Control		
Name	Specifies the name of the policy that allows or denies users access to the resource.	Enter the name.
Action	Allows or denies user access to resource.	Select Allow or Deny from the Action drop-down list.
Read-only	Allows users to view but not edit the specified resource.	Select the Read-only check box to enable this option.
Resources	Specifies the resource name for which this policy applies.	Enter the resource name.
Autopolicy:Windows File Compression		
Name	Specifies the name of the policy that allows you to compress data from the specified resource.	Enter a name.
Action	Allows you to compress data from the specified resource.	Select any one of the following options: <ul style="list-style-type: none"> • Compress—Compresses data from the specified resource. • Do not compress—Disables compression for the specified resource.
Resources	Specifies the resource names for which this policy applies.	Enter the names.
Autopolicy:Windows Server Single Sign-On		

Table 27: Configuring File Rewriting Resource Profiles Details (*continued*)

Option	Function	Your Action
New Resources	Specifies the resource policy to which this policy applies.	Enter the resource using the format: \\server[\\share[\\path]].
Action	Specifies the type of credentials to pass to the Windows share or directory.	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • Use Specified Credentials(Variable Password)...—Secure Access device uses specified credentials with variable password to pass to the Windows share or directory. • Use Specified Credentials(Fixed Password)...—Secure Access device uses specified credentials with fixed password to pass to the Windows share or directory. • Prompt for user credentials—Secure Access device intermediates the share challenge by presenting an authentication challenge in the Secure Access device the first time a user attempts to access the share. The user enters the credentials and the credentials are stored in the Secure Access device. If the credentials later fail, the Secure Access device again prompts the user for the credentials.
Username	Specifies a username to submit to the Windows share or directory.	<p>Enter a variable. For example, <USERNAME> or a static username. For example enter administrator to submit to the Windows share or directory.</p> <p>NOTE: When entering a variable, you may also include a domain. For example, yourcompany.net\\<USERNAME></p>
Variable Password	Specifies a variable password to the Windows share or directory.	Enter the variable password.
Password	Specifies a static password to the Windows share or directory.	Enter the static password.
Bookmarks		
Name	Specifies the name of the bookmark.	Enter a name.
Description	Describes the bookmark.	Enter the description.
Server	Specifies the server name.	Enter the server name.
Share	Specifies the share name.	Enter the share name.

Table 27: Configuring File Rewriting Resource Profiles Details (*continued*)

Option	Function	Your Action
Path	Adds a suffix to the resource if you want to create links to subdirectories of the resource defined in the primary resource profile.	Enter a suffix to the resource.
Appearance	Displays the bookmark on a user's welcome page and when browsing network files.	Select one of the following options: <ul style="list-style-type: none"> • Appear as bookmark on homepage and file browsing—Bookmark appears on both a user's welcome page and when browsing network files. • Appear in file browsing only—Bookmark appears only when users are browsing network files.
Applies to roles	Specifies the roles to which you want to display the bookmark.	Select one of the following options: <ul style="list-style-type: none"> • All File Profile roles—Bookmark appears both on a user's welcome page and when browsing network files. • Subset of File Profile roles—Bookmark appears only when users are browsing network files.
` Bookmarks > Role Selections		
Roles Selections	Specifies the roles to which the resource profile applies. NOTE: The Role Selections tab is enable only when you select the Subset of File Profile roles option from the Applies to roles drop-down list.	Select the role, and then click Add .

Related Documentation

- [Configuring Windows Terminal Services \(NSM Procedure\) on page 124](#)
- [Configuring a Telnet/SSH Resource Profile \(NSM Procedure\) on page 129](#)
- [Configuring Custom Web Applications Resource Profile \(NSM Procedure\) on page 112](#)

Configuring Windows Terminal Services (NSM Procedure)

Windows terminal services resource profile enables access to a Windows terminal server using an RDP client.

To configure a windows terminal service resource profile:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to windows terminal service resource profile.
2. Click the **Configuration** tab, and select **Users > Resource Profiles > Terminal Services**. The corresponding workspace appears.
3. Click the **New** button and the New dialog box appears.
4. Add or modify settings as specified in [Table 28 on page 124](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 28: Configuring Windows Terminal Services Resource Profile Details

Option	Function	Your Action
Settings tab		
Name	Specifies the name for the resource profile that becomes the default session bookmark's name.	Enter the name.
Description	Describes the bookmark.	Enter the description.
Java Support Options	Allows you to enable or disable Java applet support.	Select one of the following option: <ul style="list-style-type: none"> • Disable Java Support—Disables Java Support to intermediate traffic. • Use Java applet as a fallback mechanism—Enables the Secure Access device to fall back to the applets when other terminal services clients are not available on the user's system. • Always use Java applet—Stores terminal services Java clients directly on the Secure Access device without employing a separate Web server to host them. You can then associate these Java applets with the resource profile and specify that the Secure Access device always use them to intermediate traffic.
Applet to use	Specifies the Java applet to associate with the resource profile.	Select a Java applet from the Applet to use drop-down list.

Table 28: Configuring Windows Terminal Services Resource Profile Details (continued)

Option	Function	Your Action
Applet HTML	Specifies the HTML page definition that includes references to your Java applets.	Enter the HTML page definition. NOTE: The maximum size of the HTML that can be specified is 25 KB.
Type	Specifies the type of terminal services.	Select Windows Terminal Services to enable this feature.
Settings tab		
Host	Specifies the hostname or IP address of the Windows terminal server or metaframe terminal server.	Enter a hostname or IP address.
Server Port	Specifies the port on which the terminal server listens in the server port box.	Enter the port.
Create an access control policy	Allows you to access the server specified in the Server Port box (enabled by default).	Select the Create an access control policy check box to enable this feature.
Bookmarks tab		
Name	Specifies the name of the session bookmark.	Enter the name.
Description	Describes the session bookmark.	Enter a description.
Host	Specifies the existing host of the resource profile that connects to a Windows terminal server on the Secure Access device.	The Secure Access device automatically populates the Host and Server Port boxes using settings from the selected resource profile.
Server Port	Specifies the existing server port of the resource profile that connects to a windows terminal server on the Secure Access device.	The Secure Access device automatically populates the Host and Server Port boxes using settings from the selected resource profile.
Screen Size	Specifies the size of the terminal services window on the user's workstation.	Select the screen size from the drop-down list. NOTE: By default, the Secure Access device sets the window size to full screen.
Color Depth	Specifies the color depth of the terminal session data.	Select color depth from the drop-down list. NOTE: By default, the Secure Access device sets the color depth to 8-bit.

Table 28: Configuring Windows Terminal Services Resource Profile Details (continued)

Option	Function	Your Action
Username	Specifies the username that the Secure Access device should pass to the terminal server.	Enter the username.
Password Type	Specifies a static or variable password. If you select a variable password, then you can use the password stored in the Secure Access device's primary or secondary authentication server, or you can use the domain credentials to pass the user's cached domain credentials to the Windows Terminal server.	Select either Variable Password or Password from the Password Type drop-down list.
Variable Password	Specifies the variable password.	Enter the <password> variable. Or use the following syntax to submit the password for the secondary authentication server: <Password@SecondaryServerName> or <Password[2]>.
Explicit Password	Specifies the explicit password.	Enter the explicit password.
Launch Seamless Window	Enables the Windows application server to manage the display of the application. This allows an application's windows to behave in the same way as an application running on a Windows application server, regardless of the user's desktop environment.	Select the Launch Seamless Window check box to enable this feature.
Alias Name	Specifies the alias name (applicable only for servers running Windows 2008 and later). NOTE: This text box appears only when you select the Launch Seamless Window check box.	Enter the alias name.
Path to application	Specifies the path where the application's executable file resides on the terminal server.	Enter the path. For example, you might enter the following directory for the Microsoft Word application: C:\Program Files\Microsoft Office\Office10\WinWord.exe.

Table 28: Configuring Windows Terminal Services Resource Profile Details (continued)

Option	Function	Your Action
Working directory	Specifies where the terminal server should place working files for the application in the Working directory box.	Enter the path. For example, you might specify that Microsoft Word should save files to the following directory by default: C:\Documents and Settings\username\My Documents.
Auto-launch	Allows you to automatically launch this Terminal Service session bookmark when users sign into the Secure Access device.	Select the Auto-launch check box to enable this option.
Connect drives	Allows you to connect the user's local drive to the terminal server, enabling the user to copy information from the terminal server to his local client directories.	Select the Connect drives check box to enable this option.
Connect printers	Allows you to connect the user's local printers to the terminal server, enabling the user to print information from the terminal server to his local printer.	Select the Connect printers check box to enable this option.
Connect COM Ports	Allows you to connect the user's COM ports to the terminal server, allowing communication between the terminal server and the devices on his serial ports.	Select the Connect COM Ports check box to enable this option.
Allow Clipboard Sharing	Allows the contents of the clipboard to be shared between the user's host computer and the terminal server.	Select the Allow Clipboard Sharing check box to enable this option.
Connect smart cards	Allows users to use smart cards to authenticate their remote desktop sessions.	Select the Connect smart cards check box to enable this option.
Sound Options	Allows sound during the remote session.	Select one of the following options: <ul style="list-style-type: none"> • Disable Sound Options—Disables the sound option. • Bring to this computer—Redirects audio to the local computer. • Leave at remote computer—Plays the audio only at the server.

Table 28: Configuring Windows Terminal Services Resource Profile Details (continued)

Option	Function	Your Action
Applies to roles	Specifies the roles to which you want to display the session bookmarks.	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • All Terminal Service Profile roles—Displays the session bookmark to all of the roles associated with the resource profile. • Subset of Terminal Service Profile roles—Displays the session bookmark to a subset of the roles associated with the resource profile. Then select roles from the ALL Selected Roles list and click Add to move them to the Subset of selected roles list.
Settings tab > Bookmarks tab > Experience Options		
Desktop background	Displays a wallpaper background to users. If you do not select this option, the background is blank.	Select the Desktop background check box to enable this option.
Menu and window animation	Animates the movement of windows, menus, and lists.	Select the Menu and window animation check box to enable this option.
Bitmap Caching	Improves performance by minimizing the amount of display information that is passed over a connection.	Select the Bitmap Caching check box to enable this option.
Desktop Composition (RDP 6.0 onwards)	Allows desktop composition where individual windows no longer draw directly to the screen. Instead, their drawing is redirected to video memory, which is then rendered into a desktop image and presented on the display.	Select the Desktop Composition (RDP 6.0 onwards) check box to enable this option.
Show contents of window while dragging	Shows the contents of the Windows Explorer window while users move the windows on their desktops.	Select the Show contents of window while dragging check box to enable this option.
Themes	Sets Windows themes in their terminal server windows.	Select the Themes check box to enable this option.
Font smoothing (RDP 6.0 onwards)	Makes text smoother and easier to read. This option only works on Windows Vista computers running RDP clients that are font smoothing (RDP 6.0 version 6.0 or later).	Select the Font smoothing (RDP 6.0 onwards) check box to enable this option.
Settings > Role Selections		

Table 28: Configuring Windows Terminal Services Resource Profile Details (*continued*)

Option	Function	Your Action
Roles Selections	Specifies the roles to which the resource profile applies. NOTE: The Role Selections tab is enabled only when you select the Subset of Terminal Service Profile roles check box from the Applies to roles drop down list.	Select the role, and then click Add .

Related Documentation

- [Configuring a Telnet/SSH Resource Profile \(NSM Procedure\) on page 129](#)
- [Configuring WSAM Resource Profile \(NSM Procedure\) on page 131](#)
- [Configuring File Rewriting Resource Profiles \(NSM Procedure\) on page 120](#)

Configuring a Telnet/SSH Resource Profile (NSM Procedure)

A Telnet/SSH resource profile is a resource profile that enables users to connect to internal server hosts in the clear using Telnet protocols or to communicate over an encrypted Secure Shell session through a Web-based terminal session emulation.

To configure a Telnet/SSH resource profile:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure a Telnet/SSH resource profile.
2. Click the **Configuration** tab, and select **Users > Resource Profiles > Telnet/SSH**. The corresponding workspace appears.
3. Click the **New** button and the New dialog box appears.
4. Add or modify settings as specified in [Table 29 on page 129](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 29: Configuring Telnet/SSH Resource Profile details

Option	Function	Your Action
General tab		
Type	Specifies the session type for this resource profile.	Select Telnet or SSH from the Type drop-down list.
Name	Specifies the unique name for the resource profile.	Enter the name.
Description	Specifies the description for the resource profile.	Enter a description.

Table 29: Configuring Telnet/SSH Resource Profile details (*continued*)

Option	Function	Your Action
Host	Specifies the name or IP address of the server to which this resource profile should connect.	Enter the name or IP address.
Port	Specifies the port on which the Secure Access device should connect to the server.	Enter the port or scroll to one.
Username	Specifies the static username to pass the user's credentials to the server.	Enter the static username. For example enter <username> or another Secure Access device-appropriate session variable.
Create access control policy	Allows you to enable access to the specified server.	Select the Create an access control policy check box to enable this feature.
Role Selections tab		
Role Selections	Allows you to specify the roles to which the resource profile applies.	Select the role and, then click Add .
Bookmarks tab > General tab		
Name	Specifies the name of the bookmark.	Enter the name.
Description	Describes the bookmark.	Enter the description.
Font Size	Specifies the size of the bookmark.	Enter a size from 8 to 36 pixels or scroll to the required number. (By default, the Secure Access device sets the font size to 12.)
Screen Size	Specifies the size of the server display window.	Select a size from the drop-down list.
Screen Buffer	Allows the server window to change the number of rows to display during scrolling.	Enter the value in the Screen Buffer box (By default, the Secure Access device sets the buffer at 100 rows.)
Roles	Specifies the roles to which you want to display the bookmark.	Select one of the following option: <ul style="list-style-type: none"> • All Available roles—Displays the bookmark to all of the roles associated with the resource profile. • Selected Roles—Displays the bookmark to a subset of the roles associated with the resource profile.
Bookmarks tab > Role Selections		
Role Selections	Allows you to specify the roles for which to display a bookmark. NOTE: The Role Selections tab is enabled only when you select Selected Roles option from the Applies to roles drop-down list.	Select the role, and then click Add .

- Related Documentation**
- [Configuring WSAM Resource Profile \(NSM Procedure\) on page 131](#)
 - [Configuring a File Rewriting Resource Policy \(NSM Procedure\) on page 137](#)
 - [Configuring a JSAM Resource Profile \(NSM Procedure\) on page 93](#)

Configuring WSAM Resource Profile (NSM Procedure)

You can create two types of WSAM resource profiles:

- **WSAM application resource profiles**—These resource profiles configure WSAM to secure traffic to a client/server application. When you create a WSAM application resource profile, the WSAM client intercepts requests from the specified client applications to servers in your internal network.
- **WSAM destination network resource profiles**—These resource profiles configure WSAM to secure traffic to a server. When you create a WSAM destination network resource profile, the WSAM client intercepts requests from processes running on the client that are connecting to the specified internal hosts.

To configure a WSAM application resource profile:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure user roles.
2. Click the **Configuration tree** tab, and select **Users > Resource Profiles > SAM > Client Applications**. The corresponding workspace appears.
3. Click the **New** button, the New dialog box appears.
4. Add or modify settings as specified in [Table 30 on page 131](#).
5. Click one:
 - **OK** — Saves the changes.
 - **Cancel** — Cancels the modifications.

Table 30: Configuring WSAM Resource Profile Details

Option	Function	Your Action
Settings tab		
Name	Specifies a name for the resource profile.	Enter the name.
Description	Describes the resource profile.	Enter the description.
Type	Allows you to select WSAM.	Select the WSAM option to configure a WSAM resource profile.

Table 30: Configuring WSAM Resource Profile Details (*continued*)

Option	Function	Your Action
Domain Authentication	Allows integrated Windows applications, such as file sharing, Outlook, and so on to authenticate to the domain controller when the client machine is part of a domain.	<p>Select Domain Authentication to enable this feature.</p> <p>NOTE: Before using this option, you must:</p> <ul style="list-style-type: none"> Specify domain controllers in the WSAM Destination list so that LDAP and Kerberos traffic can be proxied and sent to the device. Configure a WSAM access control list (ACL) policy to allow access to all domain controllers.

Settings tab > Autopolicy:SAM Access Control tab

Name	Specifies the name of a policy that allows or denies users access to the resource specified in the Base URL box.	Enter the name.
Resource	Specifies the resource name.	Enter the resource name.
Action	Enables you to allow or deny the users access to the server that hosts the specified application.	Select either Allow or Deny from the Action drop-down list.

Settings tab > Settings tab

Application	Specifies the application from which WSAM intermediates traffic.	<p>Select one of the following options:</p> <ul style="list-style-type: none"> Custom—You must manually enter your custom application's executable file name (such as telnet.exe). Additionally, you may specify this file's path and MD5 hash of the executable file (although it is not required that you specify the exact path to the executable). If you enter an MD5 hash value, WSAM verifies that the checksum value of the executable matches this value. If the values do not match, WSAM notifies the user that the identity of the application could not be verified and does not forward connections from the application to the IVE. Citrix NFuse—WSAM intermediates traffic from Citrix applications. Lotus Notes—WSAM intermediates traffic from the Lotus Notes fat client application. Microsoft Outlook/Exchange—WSAM intermediates traffic from the Microsoft Outlook exchange application. NetBIOS file browsing—WSAM intercepts NetBIOS name lookups in the TDI drivers on port 137.
-------------	------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Settings > Roles tab

Table 30: Configuring WSAM Resource Profile Details (*continued*)

Option	Function	Your Action
Role Selections	Allows you to specify the roles to which the resource profile applies.	Select the role, and click Add .

To configure WSAM destination network resource profile:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure a WSAM destination network resource profile.
2. Click the **Configuration** tab, and select **Users > Resource Profiles > SAM > WSAM Destinations**. The corresponding workspace appears.
3. Click the **New** button and the New dialog box appears.
4. Add or modify settings as specified in [Table 31 on page 133](#).
5. Click one:
 - **OK** — Saves the changes.
 - **Cancel** — Cancels the modifications.

Table 31: Configuring WSAM Destination Resource Profile Details

Option	Function	Your Action
Settings tab		
Name	Specifies a name for the resource profile.	Enter the name.
Description	Describes the resource profile.	Enter the description.
Allowed WSAM Servers > Network Destination	Specifies which servers you want to secure using WSAM.	Enter a hostname or IP/netmask pairs. You may include a port.
Create an access control policy	Allows access to the server specified in the Network Destination box (enabled by default).	Select the Create an access control policy check box to enable this option.
Settings > Roles tab		
Role Selections	Specifies the roles to which the resource profile applies.	Select the role, and then click Add .

Related Documentation

- [Configuring a File Rewriting Resource Policy \(NSM Procedure\) on page 137](#)
- [Configuring a JSAM Resource Profile \(NSM Procedure\) on page 93](#)

Configuring Bookmarks for Virtual Desktop Resource Profiles (NSM Procedure)

When you create a virtual desktop resource profile, the device automatically creates a bookmark that links to the server that you specified in the resource profile. The device allows you to modify this bookmark as well as create additional bookmarks to the same server.

To configure resource profile bookmarks for virtual desktop profiles:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure resource profile bookmarks for virtual desktop profiles.
2. Click the **Configuration tree** tab, and select **Users > Resource Profiles > Virtual Desktops**.
3. Click any virtual desktop profile that is already created.
4. Click the **Bookmark** tab to modify an existing session bookmark. Or, click **New Bookmark** to create an additional session bookmark.
5. Modify the settings as described in [Table 32 on page 134](#).
6. Click **OK** to save the changes.

Table 32: Bookmarks for Virtual Desktop Resource Profile Details

Options	Your Action
Name	Enter the session bookmark name.
Description	Enter the session bookmark description.
Desktops	Select All Desktops or Subset of selected Desktops from the drop-down list. The option selected would be available to the user. The desktop list is retrieved from the connection broker using the credentials defined in the profile resource page.
Username	Enter the username for the bookmark session.
Password Type	Select Variable Password or Password from the drop-down list as the password type.
Variable Password	Enter a variable password. This option gets enabled only when you choose Variable Password as the password type.
Explicit Password	Enter an explicit password. This option gets enabled only when you choose Password as the password type.
Preferred Client	Select Automatic Detection , Citrix Client , or Java from the drop-down list as the preferred client.
Session Reliability and Auto-client reconnect	Select the check box to automatically reconnect the session reliability.
Screen Size	Select any value from the drop-down list to set the screen size.

Table 32: Bookmarks for Virtual Desktop Resource Profile Details (*continued*)

Options	Your Action
Color Depth	Select any value from the drop-down list to set the color depth.
Connect drives	Select the check box to allow users to access local resources such as drives, through the terminal session.
Connect printers	Select the check box to allow users to access local resources such as printers through the terminal session.
Connect COM Ports	Select the check box to allow users to access local resources such as COM ports through the terminal session.
Applies to roles	<p>Specify the roles to which you want to display the session bookmarks, if you are configuring the session bookmark through the resource profile pages. Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • All Virtual Desktops Profile roles—Displays the session bookmark to all of the roles associated with the resource profile. • Subset of Virtual Desktops Profile roles—Displays the session bookmark to a subset of the roles associated with the resource profile. Upon selecting this option, the Role Selections tab is enabled. Select roles from the Members list and click Add/remove to move them to the Non-members list.

- Related Documentation**
- [Configuring WSAM Resource Profile \(NSM Procedure\) on page 131](#)
 - [Configuring a Telnet/SSH Resource Profile \(NSM Procedure\) on page 129](#)

CHAPTER 10

Configuring Secure Access Resource Policies


- [Configuring a File Rewriting Resource Policy \(NSM Procedure\) on page 137](#)
- [Configuring a Secure Application Manager Resource Policy \(NSM Procedure\) on page 143](#)
- [Configuring a Telnet and Secure Shell Resource Policy \(NSM Procedure\) on page 146](#)
- [Configuring a Terminal Service Resource Policy \(NSM Procedure\) on page 148](#)
- [Configuring Web Rewriting Resource Policies \(NSM Procedure\) on page 151](#)
- [Configuring a Network Connect Connection Profile Resource Policy \(NSM Procedure\) on page 155](#)
- [Defining Network Connect Split Tunneling Policies \(NSM Procedure\) on page 159](#)

Configuring a File Rewriting Resource Policy (NSM Procedure)


File rewriting resource policies specify which Windows resources a user may access, as well as the encoding to use when communicating with Windows and NFS file shares. When a user makes a file request, the Secure Access device evaluates the resource policies corresponding to the request, such as Windows access resource policies for a request to fetch an MS Word document (.doc file). After matching a user's request to a resource listed in a relevant policy, the Secure Access device performs the action specified for the resource.

To configure a file rewriting resource policy:


1. In the navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure a file rewriting resource policy.
2. Click the **Configuration** tab. Select **Users > Resource Policies > Files**.
3. Select a policy, and then enter the name, the description, and the resources for the policy.
4. In the Applies to roles list. Select one:
 - **All**—Applies the policy to all users.
 - **Selected**—Applies the policy only to users who are mapped to roles in the Role Selection section.

- **Except those selected**—Applies this policy to all users except for those who map to the roles in the Role Selection section.
5. Select the role, and click **Add** to move the roles from non-members to members list.
.....
- 

NOTE: The Role Selections tab is enabled only when you select **Selected** or **Except those selected** option from the Applies to roles drop-down list.

.....
6. Enter the name, and specify the resources for the detailed rules.
.....
- 

NOTE: The Detailed Rules tab is enabled only when you select the **Detailed Rules** option from the Action drop-down list.

.....
- 

NOTE: To apply detailed rules to the roles, see Step 4.

.....
7. Specify one or more expressions in the Conditions box to evaluate in order to perform the action.
 8. To specify actions and additional settings on the file rewriting policy using [Table 33 on page 138](#).
 9. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 33: Configuring File Rewriting Resource Policies Details

Option	Function	Your Action
Windows ACL > General tab		
Action	Specifies the action to access resources.	Select one of the following options from the drop-down list: <ul style="list-style-type: none"> • Allow—Allows access to the resources specified in the Members list. • Deny—Denies access to the resources specified in the Members list. • Detailed Rules—Allows you to specify one or more detailed rules for this policy.
Read-only	Prevents users from saving files on the server. NOTE: This box displays only if you select Allow in the Action drop-down list.	Select the Read-only check box to enable this feature.

Table 33: Configuring File Rewriting Resource Policies Details (*continued*)

Option	Function	Your Action
Windows ACL > Detailed Rules tab		
Action	Specifies the action to perform if the user request matches a resource in the Resources list.	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • Allow—Allows the user access to the resource. • Deny—Denies the user access to the resource.
Read-only	<p>Prevents users from saving files on the server.</p> <p>NOTE: This box is enabled only when you select Allow from the Action drop-down list.</p>	Select the Read-only check box to enable this feature.
Windows SSO > General tab		
Action	Specifies the action to take when a resource requires credentials.	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • Use Specified Credentials(Variable Password)...—Secure Access device uses specified credentials with variable password to pass to the Windows share or directory • Use Specified Credentials(Fixed Password)...—Secure Access device uses specified credentials with fixed password to pass to the Windows share or directory. • Prompt for user credentials—Secure Access device intermediates the share challenge by presenting an authentication challenge in the Secure Access device the first time a user attempts to access the share. • Detailed Rules—Specifies one or more detailed rules for this policy.

Table 33: Configuring File Rewriting Resource Policies Details (*continued*)

Option	Function	Your Action
Username	<p>Specifies a username to submit to the Windows share or directory.</p> <p>NOTE: This box is enabled only when you select the Use Specified Credentials (Variable Password)... or Use Specified Credential (Fixed Password)... options from the Action drop-down list.</p>	<p>Enter a variable. For example enter <USERNAME> or a static username. For example, administrator to submit to the Windows share or directory.</p> <p>NOTE: When entering a variable, you may also include a domain. For example enter yourcompany.net\<USERNAME></p>
Variable Password	<p>Specifies a variable password to Windows share or directory.</p> <p>NOTE: This box is enabled only when you select the Use Specified Credentials (Variable Password)... option from the Action drop-down list.</p>	Enter the variable password.
Fixed Password	<p>Specifies a static password to the Windows share or directory.</p> <p>NOTE: This box is enabled only when you select the Use Specified Credential (Fixed Password)... option from the Action drop-down list.</p>	Enter the static password.
Windows SSO > Detailed Rules tab		

Table 33: Configuring File Rewriting Resource Policies Details (*continued*)

Option	Function	Your Action
Action	Specifies the action to take when a resource requires credentials.	<p>Select one of the following from the drop-down list:</p> <ul style="list-style-type: none"> • Use System Credentials...—Secure Access device submits the stored credentials to resources. • Use Specified Credentials(Variable Password)...—Secure Access device uses specified credentials with variable password to pass to the Windows share or directory • Use Specified Credentials(Fixed Password)...—Secure Access device uses specified credentials with fixed password to pass to the Windows share or directory. • Prompt for user credentials—Secure Access device intermediates the share challenge by presenting an authentication challenge in the Secure Access device the first time a user attempts to access the share. • Detailed Rules—Specifies one or more detailed rules for this policy.
Username	<p>Specifies a username to submit to the Windows share or directory.</p> <p>NOTE: This box is enabled only when you select the Use Specified Credentials(Variable Password)... or Use Specified Credential(Fixed Password)... options from the Action drop-down list.</p>	<p>Enter a variable. For example enter <USERNAME> or a static username. For example enter administrator to submit to the Windows share or directory.</p> <p>NOTE: When entering a variable, you may also include a domain. For example enter yourcompany.net\<USERNAME></p>

Table 33: Configuring File Rewriting Resource Policies Details (*continued*)

Option	Function	Your Action
Variable Password	Specifies a variable password to the Windows share or directory. NOTE: This box is enabled only when you select the Use Specified Credentials(Variable Password)... option from the Action drop-down list.	Enter the variable password.
Fixed Password	Specifies a static password to the Windows share or directory. NOTE: This box is enabled only when you select the Use Specified Credential(Fixed Password)... option from the Action drop-down list.	Enter the static password.
Windows Compression		
Action	Specifies the action you want to perform to allows or deny access to the resources.	Select one of the following options from the drop-down list: <ul style="list-style-type: none"> • Compress—Secure Access device compresses the supported content types from the specified resource. • Do not compress—Secure Access device does not compress the supported content types from the specified resource. • Use Detailed Rules—Specifies one or more detailed rules for this policy.
File Policy Options		
IP based matching for Hostname based policy resources	Secure Access device compares the IP to its cached list of IP addresses to determine if a host name matches an IP address. If there is a match, then the Secure Access device accepts the match as a policy match and applies the action specified for the resource policy.	Select the IP based matching for Hostname based policy resources check box to enable this feature.

Table 33: Configuring File Rewriting Resource Policies Details (*continued*)

Option	Function	Your Action
Case sensitive matching for the path component in File resources	Requires users to enter a case-sensitive path component.	Select the Case sensitive matching for the path component in File resources check box to enable this feature.
Encoding	Specifies the encoding to use when communicating with Windows and NFS file shares.	Select from the drop-down list.
NTLM Version	Specifies NTLM for file share authentication.	Select one of the following options from the drop-down list: <ul style="list-style-type: none"> • NTLM v1—Uses only NTLM V1 for file share authentication. • NTLM v2—Uses only NTLM V2 for file share authentication.
Number of NTLM authentication protocol variant attempts	Controls the number of login attempts while doing SSO.	Select either High or Low .

Related Documentation

- [Configuring SAML SSO Artifact Profile Resource Policy \(NSM Procedure\) on page 226](#)
- [Configuring a SAML Access Control Resource Policy \(NSM Procedure\) on page 223](#)

Configuring a Secure Application Manager Resource Policy (NSM Procedure)

When you enable the secure application manager access feature for a role, you need to create resource policies that specify which application servers a user may access. These policies apply to both the Java version and the Windows version of the Secure Application Manager (JSAM and WSAM, respectively). When a user makes a request to an application server, the Secure Access device evaluates the SAM resource policies. If the Secure Access device matches a user's request to a resource listed in a SAM policy, the Secure Access device performs the action specified for the resource.

To configure Secure Application Manager resource policy:

1. In the navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure a Secure Application Manager resource policy.
2. Click the **Configuration** tab. Select **Users > Resource Policies > SAM**.
3. Add or modify settings as specified in [Table 34 on page 144](#).
4. Click one:

- **OK**—Saves the changes.
- **Cancel**—Cancels the modifications.

Table 34: Secure Application Manager Resource Policy Configuration Details

Option	Function	Your Action
Access Control > General tab		
Name	Specifies the name for the policy.	Enter the name.
Description	Describes the policy.	Enter a description.
New Resources	Specifies the servers to which this policy applies.	Enter the server path.
Applies to roles	Specifies the roles to which this policy applies.	Select one of the following options from the drop-down list: <ul style="list-style-type: none"> • All—Applies the policy to all users. • Selected—Applies the policy only to users who are mapped to roles in the Role Selection section. • Except those selected—Specifies one or more detailed rules for this policy.
Action	Allows or denies access to the servers specified in the resources list.	Select one of the following options from the drop-down list. <ul style="list-style-type: none"> • Allow socket access—Allows access to the application servers specified in the Resources list. • Deny socket access—Denies access to the servers specified in the Resources list. • Detailed Rules—Allows you to specify one or more detailed rules for this policy.
Role Selections tab		
Role Selections	Maps roles to access resources. NOTE: This tab is enabled only when you select selected or Except those selected from the Applies to the role drop-down list.	Select a role and click Add to add roles from Non-members to Members list.
Detailed Rules tab		
Name	Specifies the detailed rule name. NOTE: The Detailed Rules tab is displayed only when you select the Detailed Rules option from the Action drop-down list.	Enter a name.

Table 34: Secure Application Manager Resource Policy Configuration Details (*continued*)

Option	Function	Your Action
Action	Specifies the action you want to perform if the user request matches a resource in the resource list (optional).	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • Allow socket access—Allows the user to access the resource. • Deny socket access—Denies the user to access the resource.
New Resources	Specifies the resource to which detailed rule applies.	<p>Specify any one of the following:</p> <ul style="list-style-type: none"> • The same or a partial list of the resources specified on the General tab. • A specific path or file on the server(s) specified on the General tab, using wildcards when appropriate. • A file type, preceded by a path if appropriate or just specify <code>*/*.file_extension</code> to indicate files with the specified extension within any path on the server(s) specified on the General tab.
Conditions	Specifies one or more expressions to evaluate to perform the action.	<p>Specify one of the following options:</p> <ul style="list-style-type: none"> • Boolean expressions: Using system variables, write one or more Boolean expressions using the NOT, OR, or AND operators. • Custom expressions: Using the custom expression syntax, write one or more custom expressions.
Options		
IP based matching for Hostname based policy resources	Secure Access device compares the IP to its cached list of IP addresses to determine if a host name matches an IP address. If there is a match, then the Secure Access device accepts the match as a policy match and applies the action specified for the resource policy.	Select Options > IP based matching for Hostname based policy resources option to enable this feature.

Related Documentation

- [Configuring a Telnet and Secure Shell Resource Policy \(NSM Procedure\) on page 146](#)
- [Configuring a Terminal Service Resource Policy \(NSM Procedure\) on page 148](#)

Configuring a Telnet and Secure Shell Resource Policy (NSM Procedure)

When you enable the Telnet/SSH access feature for a role, you need to create resource policies that specify which remote servers a user may access. If the Secure Access device matches a user's request to a resource listed in a Telnet/SSH policy, the Secure Access device performs the action specified for the resource.

To configure a Telnet and secure shell resource policy:

1. In the navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure a Telnet and secure shell resource policy.
2. Click the **Configuration** tab. Select **Users > Resource Policies > Telnet/SSH**.
3. Add or modify settings as specified in [Table 34 on page 144](#).
4. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 35: Configuring Telnet and Secure Shell Resource Policy Details

Option	Function	Your Action
Access Control > General tab		
Name	Specifies the name for the policy.	Enter the name.
Description	Describes the policy.	Enter the description.
Resources	Specifies the servers to which this policy applies.	Enter the server path.
Applies to roles	Specifies the roles to which this policy applies.	Select one of the following options from the drop-down list: <ul style="list-style-type: none"> • All—Applies the policy to all users. • Selected—Applies the policy only to users who are mapped to roles in the Role Selection section. • Except those selected—Applies the policy to all users except for those who mapped to the roles in the Role Selection section.

Table 35: Configuring Telnet and Secure Shell Resource Policy Details (continued)

Option	Function	Your Action
Action	Allows or denies access to the servers specified in the Resources list.	<p>Select one of the following options from the drop-down list.</p> <ul style="list-style-type: none"> • Allow—Allows access to the servers specified in the Resources list. • Deny—Denies access to the servers specified in the Resources list. • Detailed Rules—Allows you to specify one or more detailed rules for this policy.
Role Selections tab		
Role Selections	<p>Maps roles to the resource policy.</p> <p>NOTE: This Roles Selection tab is enabled only when you select Selected or the Except the selected option from the Applies to the role drop-down list.</p>	Select a role and click Add to add roles from Non-members to Members list.
Detailed Rules tab		
Name	<p>Specifies the detailed rule name.</p> <p>NOTE: This tab is enabled only when you select Detailed Rules from the Action drop-down list.</p>	Enter a name.
Action	Specifies the action you want to perform if the user request matches a resource in the Resource list (optional).	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • Allow—Allows the user to access the resource. • Deny—Denies the user to access the resource.
New Resources	Specifies the resource to which the detailed rule applies.	<p>Specify one of the following options:</p> <ul style="list-style-type: none"> • The same or a partial list of the resources specified on the General tab. • A specific path or file on the server(s) specified on the General tab, using wildcards when appropriate. • A file type, preceded by a path if appropriate or just specify <code>*/*file_extension</code> to indicate files with the specified extension within any path on the server(s) specified on the General tab.

Table 35: Configuring Telnet and Secure Shell Resource Policy Details (continued)

Option	Function	Your Action
Conditions	Specifies one or more expressions to evaluate to perform the action.	Specify one of the following options: <ul style="list-style-type: none"> Boolean expressions: Using system variables, write one or more Boolean expressions using the NOT, OR, or AND operators. Custom expressions: Using the custom expression syntax, write one or more custom expressions.
Options tab		
IP based matching for Hostname based policy resources	Allows the Secure Access device to look up the IP address corresponding to each hostname specified in a Telnet/SSH resource policy. When a user tries to access a server by specifying an IP address rather than the hostname, the Secure Access device compares the IP to its cached list of IP addresses to determine if a hostname matches an IP address. If there is a match, then the Secure Access device accepts the match as a policy match and applies the action specified for the resource policy.	Select Options > IP based matching for Hostname based policy resources to enable this feature.

- Related Documentation**
- [Configuring a Terminal Service Resource Policy \(NSM Procedure\) on page 148](#)
 - [Configuring Web Rewriting Resource Policies \(NSM Procedure\) on page 151](#)

Configuring a Terminal Service Resource Policy (NSM Procedure)

When you enable the terminal services feature for a role, you need to create resource policies that specify which remote servers a user can access.

To configure a terminal services resource policy:

1. In the navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure a terminal services resource policy.
2. Click the **Configuration** tab. Select **Users > Resource Policies > Terminal Services**.
3. Add or modify settings as specified in [Table 36 on page 149](#).
4. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 36: Configuring Terminal Service Resource Policy Details

Option	Function	Your Action
Access Control > General tab		
Name	Specifies the name for the policy.	Enter the name.
Description	Describes the policy.	Enter the description.
Resources	Specifies the servers to which this policy applies.	Enter the server path.
Applies to roles	Applies the policy to all the roles, and to the roles that are mapped and not mapped in the Role Selection section.	Select one of the following options from the drop-down list: <ul style="list-style-type: none"> • All—Applies the policy to all users. • Selected—Applies the policy only to users who are mapped to roles in the Role Selection section. • Except those selected—Applies this policy to all users except for those who map to the roles in the Role Selection section.
Action	Allows or denies access to the servers specified in the Resources list.	Select one of the following options from the drop-down list. <ul style="list-style-type: none"> • Allow—Allows access to the servers specified in the Resources list. • Deny—Denies access to the servers specified in the Resources list. • Detailed Rules—Allows you to specify one or more detailed rules for this policy.
Role Selections tab		
Role Selections	Maps roles to the resource policy. NOTE: The Role Selection tab is enabled only when you select the Selected or Except the selected option from the Applies to role drop-down list.	Select a role and click Add to add roles from Non-members to Members list.
Detailed Rules tab		
Name	Specifies the detailed rule name. NOTE: This Detailed Rules tab is enabled only when you select Detailed Rules option from the Action drop-down list.	Enter a name.

Table 36: Configuring Terminal Service Resource Policy Details (continued)

Option	Function	Your Action
Action	Specifies the action you want to perform if the user request matches a resource in the Resource list (optional).	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • Allow—Allows the user to access the resource. • Deny—Denies the user to access the resource.
New Resources	Specifies the resource to which detailed rule applies.	<p>Specify one of the following options:</p> <ul style="list-style-type: none"> • The same or a partial list of the resources specified on the General tab. • A specific path or file on the server(s) specified on the General tab, using wildcards when appropriate. • A file type, preceded by a path if appropriate or just specify <code>*/*:file_extension</code> to indicate files with the specified extension within any path on the server(s) specified on the General tab.
Conditions	Specifies one or more expressions to evaluate to perform the action.	<p>Specify one of the following options:</p> <ul style="list-style-type: none"> • Boolean expressions: Using system variables, write one or more Boolean expressions using the NOT, OR, or AND operators. • Custom expressions: Using the custom expression syntax, write one or more custom expressions.
Options		
IP based matching for Hostname based policy resources	The Secure Access device compares the IP to its cached list of IP addresses to determine if a hostname matches an IP address. If there is a match, then the Secure Access device accepts the match as a policy match and applies the action specified for the resource policy.	Select Options > IP based matching for Hostname based policy resources to enable this feature.

Related Documentation

- [Configuring Web Rewriting Resource Policies \(NSM Procedure\) on page 151](#)
- [Configuring a Secure Access ACE Server Instance \(NSM Procedure\) on page 161](#)

Configuring Web Rewriting Resource Policies (NSM Procedure)

Web access resource policies control which Web resources users can access in order to connect to the Internet, intranet, or extranet. You can deny or allow access to Web resources by URL or IP address range. For URLs, you can use the “*” and “?” wildcards to efficiently specify multiple hostnames and paths. For resources that you specify by hostname, you can also choose either HTTP, HTTPS, or both protocols.

To configure Web rewriting resource policy:

1. In the navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure a Web rewriting resource policy.
2. Click the **Configuration** tab. Select **Users > Resource Policies > Web**.
3. Select a policy that you want to configure, and then enter the name, the description, and the resources for the policy.
4. In the Applies to roles list, select one:
 - **All**—Applies the policy to all users.
 - **Selected**—Applies the policy only to users who are mapped to roles in the Role Selection section.
 - **Except those selected**—Applies this policy to all users except for those who map to the roles in the role selection section.
5. In the Action or the Authentication Type list, select any option from the drop-down list for the policy.
6. Select the role, and click **Add** to move the roles from the Non-members to Members list.



NOTE: The Role Selections tab is enabled only when you select the **Selected** or the **Except those selected** option from the Applies to roles drop-down list.

7. Enter the name, and specify the resources for the detailed rules.



NOTE: The Detailed Rules tab is enabled only when you select the **Detailed Rules** option from the Action drop-down list.



NOTE: To apply detailed rules to the roles, see Step 4.

8. Specify one or more expressions in the Conditions box to evaluate to perform the action.

9. Add or modify more settings as specified in [Table 37 on page 152](#).

10. Click one:

- **OK**—Saves the changes.
- **Cancel**—Cancels the modifications.

Table 37: Configuring Web Rewriting Resource Policy Details

Option	Function	Your Action
SSO From POST > General tab		
POST URL	Specifies the absolute URL where the application posts the user's credentials, such as: http://yourcompany.com/login.cgi.	Enter the URL, for example: http://yourcompany.com/login.cgi. NOTE: The Secure Access device does not accept wildcard characters in this field.
Deny direct login for this resource	Allows users to not access the URL directly.	Select the Deny direct login for this resource to enable this feature.
Allow multiple POSTs to this resource	Allows Secure Access device to send POST and cookie values to the resource multiple times if required.	Select the Allow multiple POSTs to this resource to enable this feature.
POST Variables > Label		
Label	Specifies the label that appears on a user's preferences page in the Secure Access device.	Enter the label name. NOTE: This field is required if you either enable or require users to modify data to post to back-end applications.
Name	Specifies the name to identify the data of the value box.	Enter the name. NOTE: The back-end application should expect this name.
Value	Specifies the value to post to the form for the specified name.	Enter the value. NOTE: You can enter static data, a system variable or Secure Access device session variables containing username and password values.
User Modifiable	Allows you to enable user to change the information in the value box.	Select any of the values from the drop-down list.
SSO Cookies/Headers > General tab		
Headers and Values> Header name	Specifies the text for the Secure Access device to send as header data.	Enter the text.
Headers and Values> Value	Specifies the value for the specified header.	Enter the value.

Table 37: Configuring Web Rewriting Resource Policy Details (*continued*)

Option	Function	Your Action
Caching > Options tab		
Client should cache all images less than (in KB):	Specifies the size of the image. Images are cached if it is less than the specified size.	Enter the size in KB.
Selective Rewriting > General tab		
Rewrite As	Allows Secure Access device to rewrite the content as if it were the file type.	Select any one value from the drop-down list.
Passthrough Proxy.		
Application	Specifies the application name.	Enter the name.
Description	Describes the application.	Enter the description.
URL	Specifies the application server hostname and the port used to access the application internally.	Enter the server hostname and the port. NOTE: Note that you cannot enter a path in this field.
Use virtual hostname	Allows you to specify a host name alias for the application server.	Enter the hostname name alias.
Use IVE port	Allows Secure Access device to listen for client requests to the application server on the specified Secure Access device port.	Specify a unique Secure Access device port in the range 11000-11099.
Rewrite XML	Allows Secure Access device to rewrite URLs contained within XML content.	Select the Rewrite XML to enable this feature.
Rewrite external links	Allows Secure Access device to rewrite all URLs.	Select the Rewrite external links to enable this feature.
Block cookies from being sent to the browser	Allows Secure Access device to block cookies destined for the client's browser.	Select the Block cookies from being sent to the browser to enable this feature.
Host-Header forwarding	Allows Secure Access device to pass the hostname as part of the host header instead of the actual host identifier.	Select the Host-Header forwarding check box to enable this feature.
ActiveX Parameters		
Class Id	Specifies class ID of the ActiveX control that you want to control with the policy.	Enter the class ID.

Table 37: Configuring Web Rewriting Resource Policy Details (*continued*)

Option	Function	Your Action
Description	Describes the policy.	Enter the description.
Parameters > Parameter	Specifies the ActiveX parameters that you want to control with the policy.	Enter the parameters.
Rewriting Filter		
Bug	Specifies the bug created for the device.	Enter the bug information.
Description	Describes about the bug.	Enter the description for the bug.
Enabled	Specifies if the bug needs to be filtered.	Select Enabled to enable this feature.
Web Proxy > Web Proxy Servers tab		
Name	Specifies the name or IP address of the Web proxy server and the port number at which the proxy server listens.	Enter the name or IP address.
Host	Specifies the hostname of the Web proxy server.	Enter the hostname.
Port	Specifies the port number at which the proxy server listens.	Enter the port.
Web Proxy > Web Proxy Policies > General tab		
Server	Specify a Web proxy server that you have defined. NOTE: This field is enabled only when you select Access web resources through web proxy from the Action drop-down list.	Enter or select a Web proxy server from the drop down list.
Options		
IP based matching for Hostname based policy resources	Allows Secure Access device to look up corresponding to each host name specified in a Web resource policy.	Select the IP based matching for Hostname based policy resources to enable this feature.
Case sensitive matching for the Path and Query string components in Web Resources	Allows you to require users to enter a case-sensitive URL to a resource.	Select the Case sensitive matching for the Path and Query string components in Web Resources to enable this feature.

- Related Documentation**
- [Configuring a Secure Access ACE Server Instance \(NSM Procedure\) on page 161](#)
 - [Configuring a File Rewriting Resource Policy \(NSM Procedure\) on page 137](#)

Configuring a Network Connect Connection Profile Resource Policy (NSM Procedure)

Use the Network Connect (NC) Connection Profiles tab to create an NC resource profile. When a Secure Access device receives a client request to start an NC session, the device assigns an IP address to the client-side NC agent. The device assigns this IP address based on the DHCP server or IP address pool policies that apply to a user's role. In addition, this feature allows users to specify the transport protocol, encryption method, and whether or not to employ data compression for the NC session.

To configure an NC connection profile:

1. In the navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure a NC connection profile.
2. Click the **Configuration** tab. Select **Users > Resource Policies > Network Connect > NC Connection Profile**.
3. Click **New** and then enter the name and the description for the NC connection profile.
4. Add or modify more settings as specified in [Table 38 on page 155](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
6. On the **NC Connection Profiles** page, users can prioritize the profiles to show how the device needs to be evaluated.

Table 38: Configuring Network Connect Connection Profile Details

Options	Your Action
General tab	
Name	Enter a name for the NC connection profile.
Description	Enter a description for the NC connection profile.
Transport	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • ESP (maximize performance) —This option uses a UDP encapsulated ESP transfer method to securely transfer data between the client and the device. <p>NOTE: ESP is not supported on FIPS 4500/6500 appliances. You must use oNCP/NCP. Even if you select ESP on a FIPS 4500/6500 appliance it will use oNCP/NCP.</p> <ul style="list-style-type: none"> • oNCP/NCP (maximize compatibility) —This option uses the standard oNCP/NCP transport method for this connection profile.

Table 38: Configuring Network Connect Connection Profile Details (*continued*)

Options	Your Action
UDP Port	Enter a value for the UDP port to customize the data transfer parameters. This option provides the device port through which you intend to direct UDP connection traffic. The default port number is 4500.
ESP-to-NCP fallback time-out (seconds)	Enter a value for the ESP-to-NCP fallback time-out. This option provides a period of time (in seconds) to fall back to the NCP connection already established following UDP connection failure. The default time period is 15 seconds.
Key lifetime (time based) (minutes)	Enter a value for the key lifetime. This option provides the period of time (in minutes) the device continues to employ the same ESP encryption key for this connection profile. Both the local and remote sides of the encrypted transmission tunnel use the same encryption key only for a limited period of time to help prevent unauthorized access. The default time period is 20 minutes.
Key lifetime (bytes transferred) (minutes)	Enter a value for the key lifetime for the bytes that are transferred. The default value is 0.
Replay Protection	Select the check box to enable this option. When enabled, this option helps protect against hostile “repeat attacks” from the network.
Encryption	<p>Specify the encryption method by choosing one of the following:</p> <ul style="list-style-type: none"> • AES128/MD5 (maximize performance) —This option instructs the device to employ Advanced Encryption Standard (AES) 128-bit encryption on the data channel and the MD5 authentication method for Network Connect sessions. • AES128/SHA1 —This option instructs the device to employ AES 128-bit encryption on the data channel and the SHA1 authentication method during Network Connect sessions. • AES256/MD5 —This option instructs the device to employ AES 256-bit encryption on the data channel and the MD5 authentication method for Network Connect sessions. • AES256/SHA1 (maximize security) —This option instructs the device to employ AES 256-bit encryption on the data channel and the SHA1 authentication method during Network Connect sessions.
Compression	Select No Compression from the drop-down list if you do not want to employ compression for the secure connection.
Applies to roles	Select Selected from the drop-down list if you want to select roles for the connection profile. Upon selection, the Role Selections tab is enabled.
IP Allocation tab	

Table 38: Configuring Network Connect Connection Profile Details (*continued*)

Options	Your Action
IP Address Assignment	<p>Specify the method of client-side IP address assignment. Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • DHCP server—This option allows you to specify the hostname or IP address of a network Dynamic Host Configuration Protocol (DHCP) server responsible for handling client-side IP address assignment. By default, the client's hostname is sent by the device to the DHCP server in the DHCP hostname option (option12.) Passing the user ID in the DHCP hostname option is no longer supported. As an alternative, you can configure the following entry in the DHCP options table: <i>option number=12, option value=<username><authmethod>, option type=String.</i> Or you can pass a value by adding an entry in the DHCP options table for hostname with whatever value you want. For example: <i>option number=12, option value=foo, option type=String.</i> <p>NOTE: The Secure Access device does not send a DHCP release to the DHCP server after the Network Connect session terminates.</p> <ul style="list-style-type: none"> • IP Pool—This option allows you to specify IP addresses or a range of IP addresses for the device to assign to clients that run the Network Connect service. Use the canonical format: <i>ip_range</i>. IP address pool also supports attribute substitution. For example, you can enter a RADIUS role-mapping attribute in this field, such as <i><userAttr.Framed-IP-Address></i>.
DNS tab	
Custom DNS settings	Select this option to enable the DNS setting options. Upon selecting this option, the DNS settings box gets enabled.
DNS Settings	<p>Select of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • Custom DNS Settings—This option sends the custom device DNS settings. • DHCP DNS Settings—This option sends the values the DHCP server sends to the device.
Primary DNS	Enter the IP address for the primary DNS.
Secondary DNS	Enter the IP address for the secondary DNS.
DNS Domain(s)	Enter the DNS domain(s), such as "yourcompany.com", "yourcompany.net".
WINS	Enter the WINS resolution name or IP address.
Auto-allow IP's in DNS/WINS settings (only for split-tunnel enabled mode)	Select this check box if you want to create an allow rule for the DNS server.
DNS search order	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • Search client DNS first, then the device. • Search the device's DNS servers first, then the client.
Proxy tab	

Table 38: Configuring Network Connect Connection Profile Details (*continued*)

Options	Your Action
Network Connect proxy server configuration	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • No proxy server—Specifies that the new profile requires no proxy server. • Automatic (URL for PAC file on another server)—Specifies the URL of the server on which the PAC file resides, and the frequency (in minutes) with which Network Connect polls the server for an updated version of the PAC file. • Manual configuration—Specifies the IP address or the hostname of the server and provides the port assignment.
PAC Server Address	Enter the PAC server address. This option is enabled only when you select Automatic (URL for PAC file on another server) from the Network Connect proxy server configuration option.
PAC Update Frequency (minutes)	Enter the PAC update frequency. The default value is 10.
Static Proxy Server	Enter the static proxy server address. This option is enabled only when you select Manual configuration from the Network Connect proxy server configuration option.
Static Proxy Port	Enter the static proxy port value. The default value is 0.
Roles Selection tab	
Roles Selections	Select the members from the Members list. You can add or remove the non-members to members by using the Add/Remove options.

- Related Documentation**
- [Configuring Web Rewriting Resource Policies \(NSM Procedure\) on page 151](#)
 - [Defining Network Connect Split Tunneling Policies \(NSM Procedure\) on page 159](#)

Defining Network Connect Split Tunneling Policies (NSM Procedure)

Network Connect (NC) split tunneling policies specify one or more network IP address/netmask combinations for which the device handles traffic passed between the remote client and the corporate intranet. You can also specify traffic that should not pass through the NC tunnel.

When split-tunneling is used, NC modifies routes on clients so that traffic meant for the corporate intranet networks to NC and all other traffic goes through the local physical adapter. The IVE tries to resolve all DNS requests through the physical adapter first and then routes those that fail to the NC adapter.

For example,

- If split tunneling is disabled and the exclude route contains 10.204.50.0/24, then all traffic except 10.204.50.0 networks will go through NC.
- If split tunneling is enabled and the included route contains 10.204.64.0/18 and the exclude traffic contains 10.204.68.0/24, networks from 10.204.64.0/18 to 10.204.127.0/18 will pass through the NC tunnel. The 10.204.68.0/24 network will not pass through the NC tunnel.
- If split tunneling is enabled and the include route contains 10.204.64.0/24 (subnet of the excluded route), and the exclude route contains 10.204.64.0/18 (super set of the included route), then the included network's traffic will still be routed through the NC tunnel.

To write an NC split-tunneling networks resource policy:

1. In the navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to write an NC split-tunneling networks resource policy.
2. Click the **Configuration** tab. Select **Users > Resource Policies > Network Connect > Split-tunneling Networks**.
3. Click **New Profile**, and then enter the name and the description for the policy.
4. Add or modify more settings as specified in [Table 39 on page 159](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 39: Configuring Network Connect Split Tunneling Policy Details

Options	Your Action
Resources	Enter the new resource name for the split tunnel resource policy.

Table 39: Configuring Network Connect Split Tunneling Policy Details (*continued*)

Options	Your Action
Applies to Roles	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • ALL—To apply this policy to all users. • Selected—To apply this policy only to users who are mapped to roles in the Selected roles list. Upon selecting this option, the Role Selections tab is enabled. • Except those selected—To apply this policy to all users except for those who map to the roles in the Selected roles list.
Action	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • Allow—This option allows the Network IP address/netmask combinations specified in the Resources field to pass through the NC tunnel. • Detailed Rules—This option defines resource policy rules that put additional restrictions on the specified resources. Upon selecting this option, the Detailed Rules tab is enabled. • Deny—This option denies the Network IP address/netmask combinations specified in the Resources field not to pass through the NC tunnel.
Roles Selection tab	
Roles Selections	Select the members from the Members list. You can add or remove the members to the Non-members list by selecting Add , Remove , Add All , or Remove All .
Detailed Rules tab	
Name	Enter the name for the rule.
Action	<p>Select Allow or deny from the drop-down list.</p> <p>Enter the new resource name for the rule.</p>



NOTE: On the Network Connect Split Tunneling Policies page, prioritize the policies according to how you want the device to evaluate them. Once the device matches the resource requested by the user to a resource that belongs to a Resource list of a policy (or a detailed rule's), it performs the specified action and stops processing policies.

Related Documentation

- [Configuring a Network Connect Connection Profile Resource Policy \(NSM Procedure\) on page 155](#)
- [Configuring Web Rewriting Resource Policies \(NSM Procedure\) on page 151](#)

CHAPTER 11

Configuring Authentication and Directory Servers

- [Configuring a Secure Access ACE Server Instance \(NSM Procedure\) on page 161](#)
- [Creating a Custom Expression for an Authentication Server \(NSM Procedure\) on page 163](#)
- [Configuring a Secure Access Local Authentication Server Instance \(NSM Procedure\) on page 164](#)
- [Configuring a Secure Access LDAP Server Instance \(NSM Procedure\) on page 167](#)
- [Configuring a Secure Access RADIUS Server Instance \(NSM Procedure\) on page 171](#)
- [Configuring a Secure Access Anonymous Server Instance \(NSM Procedure\) on page 174](#)
- [Configuring a Secure Access eTrust SiteMinder Server Instance \(NSM Procedure\) on page 174](#)
- [Configuring a Secure Access Certificate Server Instance \(NSM Procedure\) on page 184](#)
- [Configuring a Secure Access Manual CA Certificate \(NSM Procedure\) on page 185](#)
- [Configuring a Secure Access SAML Server Instance \(NSM Procedure\) on page 188](#)
- [Configuring a Secure Access Active Directory or NT Domain Instance \(NSM Procedure\) on page 190](#)
- [Configuring a Secure Access NIS Server Instance \(NSM Procedure\) on page 193](#)

Configuring a Secure Access ACE Server Instance (NSM Procedure)

When authenticating users with an RSA ACE server, users might sign in using two methods:

- **Using a hardware token and the standard sign-in page** — The user enters the username and password in the standard sign-in page. The device then forwards the credentials to the ACE server.
- **Using a software token and the custom SoftID sign-in page** — The user browses to the SoftID custom sign-in page. Using the SoftID plug-in, the user enters his or her username and PIN. The SoftID plug-in generates a pass phrase by concatenating the user's PIN and token and passes the pass phrase to the device. For information about enabling the SoftID custom sign-in pages, see the *Custom Sign-In Pages Solution Guide*.

To configure an ACE server instance:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure an ACE server instance.
3. Click the **Configuration** tab and select **Authentication > Auth Servers**. The corresponding workspace appears.



NOTE: If you want to update an existing server instance, click the appropriate link in the Auth Server Name box and perform the Steps 5 through 8.

4. Click the **New** button. The New dialog box appears.
5. Specify a name to identify the server instance.
6. Select **ACE Server** from the **Auth Server Type** list.
7. Configure the server using the settings described in [Table 40 on page 162](#).
8. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 40: Secure Access ACE Server Instance Configuration Details

Option	Function	Your Action
ACE Settings		
ACE Port	Specifies the port of the ACE server.	Select a default port number. NOTE: The Secure Access device uses only this setting if no port is specified in the sdconf.rec file.
Config File Name	Specifies the RSA ACE/agent configuration file.	Enter the name of the config file. NOTE: You must update this file on the device anytime you make changes to the source file.
Imported on	Specifies the importing information.	Automatically pops up the imported on information and it is not editable.
Import Config File	Specifies the configuration file for importing.	Select the configuration file for importing using the browse button.
Server Catalog > Expressions tab		
name	Allows you to enter a name for the user expression in the ACE server user directory.	Enter the name.

Table 40: Secure Access ACE Server Instance Configuration Details (continued)

Option	Function	Your Action
value	Allows you to enter a value for the user expression in the ACE server user directory.	Enter the value.

Related Documentation

- [Configuring a Secure Access Local Authentication Server Instance \(NSM Procedure\) on page 164](#)
- [Configuring a Secure Access LDAP Server Instance \(NSM Procedure\) on page 167](#)
- [Creating and Configuring Secure Access Device Administrator Roles \(NSM Procedure\) on page 43](#)

Creating a Custom Expression for an Authentication Server (NSM Procedure)

Custom expressions are strings that are made up of variables, operators, and subexpressions all concatenated together. These operators and variables are provided through an expressions dictionary.

To create a custom expression for an authentication server:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure a server catalog.
3. Click the **Configuration** tab. In the configuration tree, select **Authentication > Auth Servers**.
4. Add or modify an auth server instance and then select **Server Catalog**. The Expressions tab appears.
5. Click **New** to create a custom expression. The Custom Expression editor appears. On the left side of the editor is the Expression Dictionary, which includes the following custom expression building blocks:
 - **Logical Operators:** This node consists of logical operators that are used to build expressions. Select a logical operator and click the **Insert Expression** button to insert logical operators in expressions.
 - **Prebuilt Expressions:** This node consists of expressions that function as templates for custom expressions. Select a prebuilt expression and click the **Insert Expression** button. The prebuilt expression is displayed in the Expression area. Modify the values to create your own custom expression.
 - **Variables:** This node consists of variables. When a variable is selected, the conditional operators that can be applied to this variable are listed in the center of the Custom Expressions editor. Also, some variables have extensions that are displayed in the

drop-down list next to the variable. Double-click a variable to display its description and example usage. Click the example variable to insert it in the Expression area.

- **Your Expressions:** This node consists of expressions that you created for a particular server catalog. To reuse an existing expression, select the expression and click the **Insert Expression** button.



NOTE: Refer to the *Juniper Networks Secure Access Administration Guide* for more information on variables and writing custom expressions.

6. Enter a name for the custom expression.
7. Select a variable or prebuilt expression from the Custom Dictionary, and click **Insert Expression**. The expression is displayed in the Expression area on the right side of the Custom Expression editor. The conditional operators can be selected only after a leaf node is selected.
8. Click the **Validate** button to validate the expression. The expression is validated by the device and the validation status appears.



NOTE: You can create a custom expression in a device template, but you cannot validate the custom expression. The **Validate** button is not enabled in the Custom Expressions editor of device templates.

9. Click **OK** to save the custom expression. The new custom expression is displayed under the Expressions tab of the server catalog.
10. Click **OK** to save the auth server settings.

Related Documentation

- [Creating a Custom Expression for Sensor Settings \(NSM Procedure\) on page 268](#)

Configuring a Secure Access Local Authentication Server Instance (NSM Procedure)

The Secure Access device enables you to create one or more local databases of users who are authenticated by the device. You might want to create local user records for users who are normally verified by an external authentication server that you plan to disable or if you want to create a group of temporary users. Note that all administrator accounts are stored as local records, but you can choose to authenticate administrators using an external server by creating authentication policies.

To configure a local authentication server instance:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure a local authentication server instance.
3. Click the **Configuration** tab and select **Authentication > Auth Servers**. The corresponding workspace appears.



NOTE: If you want to update an existing server instance, click the appropriate link in the Auth Server Name box and perform the Steps 5 through 8.

4. Click the **New** button. The New dialog box appears.
5. Specify a name to identify the server instance.
6. Select **Local Authentication** from the **Auth Server Type** list.
7. Configure the server using the settings described in [Table 41 on page 165](#).
8. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 41: Secure Access Local Authentication Server Instance Configuration Details

Option	Function	Your Action
Local Auth Settings		
Minimum password length (characters)	Specifies the minimum character length for passwords.	Set the minimum character length for passwords.
Maximum password length	Specifies the maximum character length for passwords. NOTE: This is optional.	Set the maximum character length for passwords. NOTE: The maximum length cannot be less than the minimum length. There is no maximum limit to the length.
Minimum number of digits required in the password (digits)	Specifies the minimum number of digits that is required in the password.	Set the minimum number of digits that is required in the password.
Minimum number of letters required in the password (letters)	Specifies the minimum number of letters that is required in the password.	Set the minimum number of letters that is required in the password.
Require password to have a mix of UPPER and LOWER CASE letters	Specifies if the password must contain both uppercase and lowercase letters.	Select Local Auth Settings > Require passwords to have a mix of UPPER and LOWER CASE letters to enable this option.
Require password to be different from username	Specifies if you want users to set the password to be different from the username.	Select Local Auth Settings > Require password to be different from username to enable this option.

Table 41: Secure Access Local Authentication Server Instance Configuration Details (*continued*)

Option	Function	Your Action
Require new passwords to be different from previous password	Specifies if you want users to set the new password to be different from the previous password.	Select Local Auth Settings > Require new passwords to be different from previous password to enable this option.
Allow users to change their passwords	Specifies that users can change their passwords.	Select Local Auth Settings > Allow users to change their passwords to enable this option.
Force user to change password (days)	Specifies the user the number of days after which the password expires.	Set the number of days after which the password expires.
Prompt user to change password (days)	Specifies the number of days before password expiration to prompt the user.	Set the number of days before password expiration to prompt the user.
Users		
Username	Specifies the username.	Enter the username.
Full name	Specifies the user's full name.	Enter the user's full name.
Password	Specifies the password.	Enter the password.
One-time user	Specifies if you want to limit the user to one login.	Select Users > One-time user to enable this option.
Enabled	This option is used by the administrator.	Select Users > Enabled to enable this option.
Require users to change password at next sign in	Specifies if you want to force users to change their password at the next login.	Select Users > Require users to change password at next sign in to enable this option.
Server Catalog > Expressions tab		
name	Specifies the name of the local authentication server instance.	Enter a name.
value	Specifies the value of the local authentication server instance.	Enter a value.

Related Documentation

- [Configuring a Secure Access LDAP Server Instance \(NSM Procedure\) on page 167](#)
- [Configuring a Secure Access RADIUS Server Instance \(NSM Procedure\) on page 171](#)
- [Configuring a Secure Access ACE Server Instance \(NSM Procedure\) on page 161](#)

Configuring a Secure Access LDAP Server Instance (NSM Procedure)

The Secure Access device supports two LDAP-specific authentication options:

- **Unencrypted**—the device sends the username and password to the LDAP Directory Service in clear and simple text.
- **LDAPS**—the device encrypts the data in the LDAP authentication session using the Secure Socket Layer (SSL) protocol before sending it to the LDAP Directory Service.

To configure an LDAP server instance:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure an LDAP server instance.
3. Click the **Configuration** tab and select **Authentication > Auth Servers**. The corresponding workspace appears.



NOTE: If you want to update an existing server instance, click the appropriate link in the Auth Server Name box and perform the Steps 5 through 8.

4. Click the **New** button. The New dialog box appears.
5. Specify a name to identify the server instance.
6. Select **LDAP Server** from the **Auth Server Type** list.
7. Configure the server using the settings described in [Table 42 on page 167](#).
8. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 42: Secure Access LDAP Server Instance Configuration Details

Option	Function	Your Action
LDAP Settings > Basic Settings tab		
LDAP Server	Specifies the name or IP address of the LDAP server that the Secure Access device uses to validate your users.	Enter the name or IP address of the LDAP server.
LDAP Port	Specifies the port on which the LDAP server responds. NOTE: This port is 389 when using an unencrypted connection and 636 when using SSL.	Set the port for the LDAP server.

Table 42: Secure Access LDAP Server Instance Configuration Details (continued)

Option	Function	Your Action
Backup LDAP Server1	Specifies the parameters for backup LDAP server1 (optional). NOTE: The device uses this type of server for failover processing. Also, backup LDAP server must be the same version as the primary LDAP server.	Enter the IP address of the backup LDAP server1. NOTE: We do not recommend entering hostname as it may accelerate failover processing by eliminating the need to resolve the hostname to an IP address.
Backup LDAP Port1	Specifies the parameters for backup LDAP port1.	Enter the port number for the backup LDAP port1.
Backup LDAP Server2	Specifies the parameters for backup LDAP server2 (optional).	Enter the IP address of the backup LDAP server2.
Backup LDAP Port2	Specifies the parameters for backup LDAP port2.	Enter the port number for the backup LDAP port2.
LDAP Server Type	Specifies the type of LDAP server that you want to authenticate users against.	Select the type of LDAP server from the drop-down list.
Connection	Specifies whether or not the connection between the Secure Access device and LDAP Directory Service should be unencrypted, use SSL (LDAPS), or should use TLS.	Select the type of connection from the drop-down list.
Connection Timeout (seconds)	Specifies how long you want the Secure Access device to wait for a connection to the primary LDAP server first, and then each backup LDAP server in turn.	Set the time required for the connection to time out.
Search Timeout (seconds)	Specifies how long you want the Secure Access device to wait for search results from a connected LDAP server.	Set the time required for the search to time out.
LDAP Settings > Authentication tab		
Authentication required to search LDAP	Specifies if the device needs to authenticate against the LDAP Directory Service to perform a search or to change passwords using the password management feature.	Select LDAP Settings > Authentication > Authentication required to search LDAP to enable this option.
Admin DN	Performs an anonymous search on the LDAP server with an authentication.	Enter the admin DN name.

Table 42: Secure Access LDAP Server Instance Configuration Details (*continued*)

Option	Function	Your Action
Password	Specifies the password for the admin DN name.	Enter the password.
LDAP Settings > Finding User Entries tab		
Base DN	Starts searching for user entries.	Enter a base DN name. For example, DC=eng, DC=Juniper, DC=com .
Filter	Fine tunes the search.	<p>Enter a filter value. For example, entersamAccountname=<username> or cn=<username>.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • Include <username> in the filter to use the username entered on the sign-in page for the search. • Specify a filter that returns 0 or 1 user DN's per user; the device uses the first DN returned if more than 1 DN is returned.
LDAP Settings > Determining Group Membership tab		
Base DN	Starts searching for user groups.	Enter a base DN name.
Filter	Fine tunes the search for a user group.	Enter a filter value.
Member Attribute	Identifies all the members of a static group.	Enter a name if you want to identify all the members of a static group. For example, enter member uniquemember (iPlanet-specific) .
Reverse group search	Starts the search from the member instead of the group.	Select LDAP Settings > Determining Group Membership > Reverse group search to enable this option.
Query Attribute	Specifies an LDAP query that returns the members of a dynamic group.	Enter a name for the query attribute. For example, enter memberURL .
Nested Group Level	Specifies how many levels within a group to search for the user.	Set the number for the search query time.
	<p>NOTE: The higher the number, the longer the query time, so we recommend that you specify to perform the search no more than two levels deep.</p>	

Table 42: Secure Access LDAP Server Instance Configuration Details (continued)

Option	Function	Your Action
Nested Group Search	<p>Specifies the types of nested group searches available. They are:</p> <ul style="list-style-type: none"> • Nested groups in Server Catalog — This option is faster because it can search within the implicit boundaries of the nested group. • Search all nested groups — With this option, the device searches the Server Catalog first. If the device finds no match in the catalog, then it queries LDAP to determine if a group member is a sub-group. 	Select any one type of nested group search from the drop-down list.
LDAP Settings > Meetings tab		
User Name	Specifies the username attribute for the LDAP server.	Enter the username for the server. For example, SamAccountName for an Active Directory server or uid for an iPlanet server.
Email Address	Specifies the e-mail attribute for the LDAP server.	Enter the e-mail address for the server.
Display Name, Attributes	Specifies if there are any additional LDAP attributes whose contents you want to allow meeting creators to view (optional).	<p>Enter a name. For example, to help the meeting creator easily distinguish between multiple invitees with the same name, you may want to expose an attribute that identifies the departments of individual users.</p> <p>NOTE: Enter the additional attributes one per line using the format: DisplayName,AttributeName. You may enter up to 10 attributes.</p>
Server Catalog > Expressions tab		
Name	Specifies the name that is used to show a list of common LDAP expressions.	Enter a name. For example, cn, uid, uniquemember , and memberof .
Value	Specifies the custom value of the LDAP server.	Enter a value for the LDAP server.
Server Catalog > Attributes tab		
Name	Specifies the name that is used to show a list of common LDAP attributes.	Enter a name for the LDAP attributes.
Server Catalog > Groups tab		

Table 42: Secure Access LDAP Server Instance Configuration Details (continued)

Option	Function	Your Action
Name	Specifies the name that is used to easily retrieve group information from an LDAP server and add it to the server's device server catalog.	Enter a name.
DN	Specifies the base DN name of the group.	Enter a base DN name. NOTE: If you do not know the exact container of your groups, you can specify the domain root as the base DN, such as dc=juniper, dc=com . The search page returns a list of groups from your server that you can use to enter into the Groups list.
Group Type	Specifies the group type.	Select any one group type from the drop-down list.

Related Documentation

- [Configuring a Secure Access RADIUS Server Instance \(NSM Procedure\) on page 171](#)
- [Configuring a Secure Access Anonymous Server Instance \(NSM Procedure\) on page 174](#)
- [Configuring a Secure Access Local Authentication Server Instance \(NSM Procedure\) on page 164](#)

Configuring a Secure Access RADIUS Server Instance (NSM Procedure)

A Remote Authentication Dial-In User Service (RADIUS) server is a type of server that allows you to centralize authentication and accounting for remote users. When using a RADIUS server to authenticate Secure Access device users, you need to configure it to recognize the Secure Access device as a client and specify a shared secret for the RADIUS server to use to authenticate the client request.

To configure a connection to the RADIUS server on the Secure Access device:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure RADIUS server instance.
3. Click the **Configuration** tab and select **Authentication > Auth Servers**. The corresponding workspace appears.



NOTE: If you want to update an existing server instance, click the appropriate link in the Auth Server Name box, and perform the Steps 5 through 8.

4. Click the **New** button. The New dialog box appears.

5. In the Auth Server Name list, specify a name for the RADIUS Server.
6. Select **Radius Server** from the Auth Server Type list.
7. Configure the server using the settings described in [Table 43 on page 172](#).
8. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 43: RADIUS Server Configuration Details

Option	Function	Your Action
Primary Server tab		
Radius Server	Specifies a unique name or IP address for the RADIUS server.	Enter the name or IP address.
NAS-Identifier	Identifies the Secure Access device network access server client that communicates with the RADIUS server.	Enter the name.
Authentication Port	Specifies the authentication port value for the RADIUS server.	Enter the port value. NOTE: Typically this port is 1812, but some legacy servers might use 1645.
Shared Secret	Specifies a string for the shared secret.	Enter a string for the shared secret.
Accounting Port	Specifies the accounting port value for the RADIUS server.	Enter the port value. NOTE: Typically this port is 1813, but some legacy servers might use 1646.
NAS-IP-Address	Controls the NAS IP address value passed to RADIUS requests.	Enter the NAS IP address.
Timeout (minutes)	Specifies the time interval for the Secure Access device to wait for a response from the RADIUS server before timing out the connection.	Enter the time.
Retries	Allows Secure Access device to try to make a connection after the first attempt fails.	Enter the number of retries.
Users authenticate using tokens or one-time passwords	Allows you not to submit the password entered by the user to other SSO enabled applications.	Select Users authenticate using tokens or one-time passwords check box.
Backup Server tab		

Table 43: RADIUS Server Configuration Details (*continued*)

Option	Function	Your Action
Backup Radius Server	Specifies a secondary RADIUS server for the Secure Access device to use if the primary server—the one defined in this instance—is unreachable.	Enter a secondary RADIUS server name or IP address.
Backup Authentication Port	Specifies the authentication port for the backup RADIUS server.	Enter the port value.
Backup Shared Secret	Specifies a string for the shared secret.	Enter a string for the shared secret.
Backup Accounting Port	Specifies the accounting port for the backup RADIUS server.	Enter the port value.
Radius Accounting tab		
User-Name	Specifies the user information that the Secure Access device should send to the RADIUS accounting server.	<p>Enter a name.</p> <p>The default variables for this field are:</p> <ul style="list-style-type: none"> • <username>—Logs the user's Secure Access device username to the accounting server. • <REALM>—Logs the user's Secure Access device realm to the accounting server. • <ROLE>—Logs the user's Secure Access device role to the accounting server. If the user is assigned to more than one role, the Secure Access device comma-separates them.
Interim Update Interval (minutes)	Enables you to accomplish more precise billing for long-lived session clients and in case of a network failure.	Enter the time.
Use NC assigned IP Address for FRAMED-IP-ADDRESS attribute	Uses the IP address returned from the Secure Access device for the framed-IP-address attribute.	Select the Use NC assigned IP Address for FRAMED-IP-ADDRESS attribute check box.

Related Documentation

- [Configuring a Secure Access Anonymous Server Instance \(NSM Procedure\) on page 174](#)
- [Configuring a Secure Access eTrust SiteMinder Server Instance \(NSM Procedure\) on page 174](#)
- [Configuring a Secure Access LDAP Server Instance \(NSM Procedure\) on page 167](#)

Configuring a Secure Access Anonymous Server Instance (NSM Procedure)

The anonymous server feature allows users to access the Secure Access device without providing a username or password. Instead, when a user enters the URL of a sign-in page that is configured to authenticate against an anonymous server, the Secure Access device bypasses the standard Secure Access device sign-in page, and immediately displays the Secure Access device welcome page to the user.

To configure an anonymous server instance:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure authentication protocol sets.
3. Click the **Configuration** tab and select **Authentication > Auth Servers**. The corresponding workspace appears.



NOTE: If you want to update an existing server instance, click the appropriate link in the Auth Server Name box and perform the Steps 5 through 8.

4. Click the **New** button. The New dialog box appears.
5. Specify a name to identify the server instance.
6. Select **Anonymous Server** from the Auth Server Type list.
7. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Related Documentation

- [Configuring a Secure Access eTrust SiteMinder Server Instance \(NSM Procedure\) on page 174](#)
- [Configuring a Secure Access Certificate Server Instance \(NSM Procedure\) on page 184](#)
- [Configuring a Secure Access RADIUS Server Instance \(NSM Procedure\) on page 171](#)

Configuring a Secure Access eTrust SiteMinder Server Instance (NSM Procedure)

Within the Secure Access device, a SiteMinder instance is a set of configuration settings that defines how the Secure Access device interacts with the SiteMinder policy server.

To configure the SiteMinder server instance:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure eTrust SiteMinder server instance.

3. Click the **Configuration** tab and select **Authentication > Auth Servers**. The corresponding workspace appears.



NOTE: If you want to update an existing server instance, click the appropriate link in the Auth Server Name box, and perform the Steps 5 through 10.

4. Click the **New** button. The New dialog box appears.
5. In the Auth Server Name list, specify a name to identify the server instance.
6. Select **SiteMinder Server** from the Auth Server Type list.
7. Configure the server using the settings described in [Table 44 on page 175](#).
8. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
9. Set advanced SiteMinder configuration options (optional) using the settings described in [Table 45 on page 182](#).

Table 44: Secure Access eTrust SiteMinder Configuration Details

Option	Function	Your Action
Siteminder Settings > Basic Settings tab		
Policy Server	Specifies the name or IP address of the SiteMinder policy server.	Enter a name or IP address.
Backup Server(s)	Specifies a list of backup policy servers (optional).	Enter a comma-delimited list of backup policy servers (optional).
Failover Mode?	Allows the Secure Access device to use the main policy server unless it fails.	<ul style="list-style-type: none"> • Select Yes — Secure Access device uses the main policy server unless it fails. • Select No— Secure Access device load balances among all the specified policy servers.
Agent Name	Specifies the SiteMinder agent name.	Enter an agent name. NOTE: Shared secret and agent name are case-sensitive.
Secret	Specifies the shared secret.	Enter a shared secret name. NOTE: Shared secret and agent name are case-sensitive.

Table 44: Secure Access eTrust SiteMinder Configuration Details (*continued*)

Option	Function	Your Action
Compatible with	Specifies a SiteMinder server version. Version 5.5 supports 5.5 and 6.0. Version 6.0 supports only 6.0 of the SiteMinder server API. The default value is 5.5 policy servers.	Select the server version from the drop-down list.
On logout, redirect to	Specifies a URL to which users are redirected when they sign out of the Secure Access device (optional). If you leave this field empty, users see the default Secure Access device sign-in page.	Enter a URL.
Protected Resource	Specifies a default protected resource. If you do not create sign-in policies for SiteMinder, the Secure Access device uses this default URL to set the user's protection level for the session. The Secure Access device also uses this default URL if you select the Automatic Sign-In option.	Enter a URL. NOTE: You must enter a forward slash (/) at the beginning of the resource (for example, enter <code>"/ive-authentication"</code>).

Siteminder Settings > SMSESSION cookie settings tab

Cookie Domain	Specifies the cookie domain of the Secure Access device.	Enter a URL for the cookie domain. NOTE: <ul style="list-style-type: none"> Multiple domains should use a leading period and be comma separated. For example: <code>.sales.myorg.com, .marketing.myorg.com</code>. Domain names are case-sensitive. You cannot use wildcard characters. For example, if you define <code>".juniper.net"</code> , the user must access the Secure Access device as <code>"http://secure access device.juniper.net"</code> to ensure that his SMSESSION cookie is sent back to the Secure Access device.
---------------	----------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Table 44: Secure Access eTrust SiteMinder Configuration Details (*continued*)

Option	Function	Your Action
IVE Cookie Domain	Specifies the internet domain(s) to which the Secure Access device sends the SMSESSION cookie using the same guidelines outlined for the Cookie Domain field.	Enter a URL.
Protocol	Sends cookies securely and non securely.	Select the protocol from the drop-down list: <ul style="list-style-type: none"> • HTTPS—Sends cookies securely if other Web agents are set up to accept secure cookies. • HTTP—Sends cookies non securely.
SiteMinder Settings > Authentication tab		
Automatic Sign-In	Allows users with a valid SMSESSION to automatically sign in to the Secure Access device.	Select the Automatic Sign-In option to enable this feature.
Automatic Sign In realm to use	Specifies an authentication realm for automatically signed-in users. The Secure Access device maps the user to a role based on the role mapping rules defined in the selected realm.	Select an authentication realm from the drop-down list.
If Automatic Sign In fails, redirect to	Specifies an alternate URL for users who sign into the Secure Access device through the Automatic Sign-In mechanism. The Secure Access device redirects users to the specified URL if the Secure Access device fails to authenticate and no redirect response is received from the SiteMinder policy server. If you leave this field empty, users are prompted to sign back in to the Secure Access device. <p>NOTE: Users who sign in through the sign-in page are always redirected back to the Secure Access device sign-in page if authentication fails.</p>	Enter a URL.

Table 44: Secure Access eTrust SiteMinder Configuration Details (*continued*)

Option	Function	Your Action
Authentication Type > Custom Agent	Authenticates using the Secure Access device custom Web agent.	Select SiteMinder Settings > Authentication > Authentication Type > Custom Agent option from the Authentication Type drop-down list.
Authentication Type > Form POST	Posts user credentials to a standard Web agent that you have already configured rather than contacting the SiteMinder policy server directly.	Select SiteMinder Settings > Authentication > Authentication Type > Form POST option from the Authentication Type drop-down list to allow the Web agent to contact the policy server to determine the appropriate sign-in page to display to the user.
Form POST Target	Specifies the target URL. NOTE: The form post target, form post protocol, form post Webagent, form post port, form post path, and form post parameters field are displayed only when you select Form POST option from the Authentication type drop down list.	Enter the target URL.
Form POST Protocol	Allows you to specify the protocol for communication between IVE and the specified Web agent. NOTE: This field is displayed only when you select the Form POST option from the Authentication Type drop-down list.	Select the protocol from the drop-down list: <ul style="list-style-type: none"> • HTTP—For non secure communication. • HTTPS—For secure communication.
Form POST Webagent	Specifies the name of the Web agent from which the Secure Access device is to obtain SMSESSION cookies. NOTE: This field is displayed only when you select Form POST option from the Authentication Type drop-down list.	Enter the name of the web agent.

Table 44: Secure Access eTrust SiteMinder Configuration Details (*continued*)

Option	Function	Your Action
Form POST Port	<p>Specifies the port for the protocol.</p> <p>NOTE: This field is displayed only when you select the Form POST option from the Authentication Type drop-down list.</p>	<p>Enter port 80 for HTTP or port 443 for HTTPS.</p>
Form POST Path	<p>Specifies the path of the sign-in page.</p> <p>NOTE: This field is displayed only when you select the Form POST option from the Authentication Type drop-down list.</p>	<p>Enter the path of the Web agent's sign-in page.</p> <p>NOTE: The path must start with a backslash (/) character. In the Web agent sign-in page URL, the path appears after the Web agent.</p>
Form POST Parameters	<p>Specifies the post parameters to be sent when a user signs in.</p> <p>NOTE: This field is displayed only when you select the Form POST option from the Authentication Type drop-down list.</p>	<p>Enter the post parameters.</p> <p>Common SiteMinder variables that you can use include <code>_USER_</code>, <code>_PASS_</code>, and <code>_TARGET_</code>. These variables are replaced by the username and password entered by the user on the Web agent's sign-in page and by the value specified in the Target field. These are the default parameters for login.fcc—if you have made customizations, you may need to change these parameters.</p>

Table 44: Secure Access eTrust SiteMinder Configuration Details (continued)

Option	Function	Your Action
Authentication Type > Delegate to a Standard Agent	Delegates authentication to a standard agent. When the user accesses the Secure Access device sign-in page, the Secure Access device determines the FCC URL associated with the protected resource's authentication scheme. The Secure Access device redirects the user to that URL, setting the Secure Access device sign-in URL as the target. After successfully authenticating with the standard agent, an SMSESSION cookie is set in the user's browser and the user is redirected back to the Secure Access device. The Secure Access device then automatically signs in the user and establishes a Secure Access session.	Select SiteMinder Settings > Authentication > Authentication Type > Delegate to a Standard Agent option from the Authentication Type drop-down list.
SiteMinder Settings > Authorization tab		
Authorize requests against SiteMinder policy server	Uses SiteMinder policy server rules to authorize user Web resource requests. If you select this option, make sure that you create the appropriate rules in SiteMinder that start with the server name followed by a forward slash, such as: "www.yahoo.com/", "www.yahoo.com/*", and "www.yahoo.com/r/fi".	Select SiteMinder Settings > Authorization > Authorize requests against SiteMinder policy server .

Table 44: Secure Access eTrust SiteMinder Configuration Details (*continued*)

Option	Function	Your Action
If authorization fails, redirect to	Specifies an alternative URL that users are redirected to if the Secure Access device fails to authorize and no redirect response is received from the SiteMinder policy server. If you leave this field empty, users are prompted to sign back in to the Secure Access device. NOTE: If you are using an authorization-only access policy, you must enter an alternative URL in this field regardless of whether the Authorize requests against SiteMinder policy server option is selected. Users are redirected to this URL when an access denied error occurs. See "Defining authorization-only access policies."	Enter a URL.
Resource for insufficient protection level	Specifies a resource on the Web agent to which the Secure Access device redirects users when they do not have the appropriate permissions.	Enter a URL.
Ignore authorization for files with extensions	Specifies file extensions corresponding to file types that do not require authorization.	Enter the extensions of each file type that you want to ignore, separating each with a comma. For example, enter .gif, .jpeg, .jpg, .bmp to ignore various image types. You cannot use wildcard characters (such as *, **, or .*) to ignore a range of file types.
Server Catalog > Expressions tab		
Name	Specifies a name for the user expression in the SiteMinder user directory.	Enter a name.
Value	Specifies a value for the user expression in the SiteMinder user directory.	Enter a value.
Server Catalog > Attributes tab		

Table 44: Secure Access eTrust SiteMinder Configuration Details (*continued*)

Option	Function	Your Action
Name	Specifies the name of the user attribute cookie in the SiteMinder user directory.	Enter a name.

Table 45: Secure Access eTrust SiteMinder Advanced Configuration Details

Option	Function	Your Action
Siteminder Settings > Advanced tab		
Poll Interval (seconds)	Specifies the interval at which Secure Access device polls the SiteMinder policy server to check for a new key.	Enter the poll interval in seconds.
Maximum Agents	Controls the maximum number of simultaneous connections that the Secure Access device is allowed to make to the policy server. NOTE: The default setting is 20.	Enter a number.
Maximum Requests/Agent	Controls the maximum number of requests that the policy server connection handles before the Secure Access device ends the connection. If necessary, tune to increase performance. NOTE: The default setting is 1000.	Enter a number.
Idle Timeout (minutes)	Controls the maximum number of minutes a connection to the policy server may remain idle (the connection is not handling requests) before the Secure Access device ends the connection. The default setting of "none" indicates no time limit.	Enter the Idle timeout in minutes.
Authorize while Authenticating	Specifies that the Secure Access device should look up user attributes on the policy server immediately after authentication to determine if the user is truly authenticated.	Select Siteminder Settings > Advanced > Authorize while Authenticating .

Table 45: Secure Access eTrust SiteMinder Advanced Configuration Details (*continued*)

Option	Function	Your Action
Siteminder Settings > Advanced tab		
Enable Session Grace Period	<p>Eliminates the overhead of verifying a user's SMSESSION cookie each time the user requests the same resource by indicating that the Secure Access device should consider the cookie valid for a certain period of time.</p> <p>If you do not select this option, the Secure Access device checks the user's SMSESSION cookie on each request.</p>	<p>Select Siteminder Settings > Advanced > Enable Session Grace Period to enable this feature.</p> <p>You can eliminate the overhead of verifying a user's SMSESSION cookie each time the user requests the same resource by indicating that the Secure Access device should consider the cookie valid for a certain period of time. During that period, the Secure Access device assumes that its cached cookie is valid rather than revalidating it against the policy server. Note that the value entered here does not affect session or idle timeout checking.</p>
Validate cookie every (seconds)	Specifies the time period for the Secure Access device to eliminate the overhead of verifying a user's SMSESSION cookie each time the user requests the same resource by indicating that the Secure Access device should consider the cookie valid for a certain period of time.	Enter the time period in seconds.
Ignore Query Data	Specifies that the Secure Access device does not cache the query parameter in its URLs. Therefore, if a user requests the same resource as is specified in the cached URL, the request should not fail.	Select the Ignore Query Data option to enable this feature.
Accounting Port	Specifies that the value entered in this field must match the accounting port value entered through the Policy Server Management Console in the web UI. By default, this field matches the policy server's default setting of 44441.	Enter the value.

Table 45: Secure Access eTrust SiteMinder Advanced Configuration Details (*continued*)

Option	Function	Your Action
Siteminder Settings > Advanced tab		
Authentication Port	The value entered in this field must match the authentication port value entered through the Policy Server Management Console. By default, this field matches the policy server's default setting of 44442.	Enter a value.
Authorization Port	The value entered in this field must match the authorization port value entered through the Policy Server Management Console. By default, this field matches the policy server's default setting of 44443.	Enter a value.

Related Documentation

- [Configuring a Secure Access Certificate Server Instance \(NSM Procedure\) on page 184](#)
- [Configuring a Secure Access SAML Server Instance \(NSM Procedure\) on page 188](#)
- [Configuring a Secure Access Anonymous Server Instance \(NSM Procedure\) on page 174](#)

Configuring a Secure Access Certificate Server Instance (NSM Procedure)

The certificate server feature allows users to authenticate based on attributes contained in client-side certificates. You may use the certificate server by itself or in conjunction with another server to authenticate users and map them to roles.

To configure certificate server instance:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure user roles.
2. Click the **Configuration** tab, and then select **System > Configuration > Certificates > Trusted Client CAs** tab to import the CA certificate used to sign the client-side certificates. The corresponding workspace appears.
3. Select **Authentication > Auth Servers**.
4. Click the **New** button. The New dialog box appears.



NOTE: If you want to update an existing server instance, click the appropriate link in the Auth Server Name box, and perform the Steps 5 through 8.

5. Specify a name to identify the server instance.

6. Select **Certificate Server** from the Auto Server Type list.
7. Configure the server using the settings described in [Table 46 on page 185](#).
8. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 46: Secure Access Certificate Configuration Details

Option	Function	Your Action
Certificate Settings		
User Name Template	Specifies how the Secure Access device should construct a username.	Enter any combination of certificate variables contained in angle brackets and plain text.
Server Catalog > Expressions tab		
Name	Specifies a name for the user expression in the certificate server user directory.	Enter a name.
Value	Specifies a value for the user expression in the certificate server user directory.	Enter a value.

Related Documentation

- [Configuring a Secure Access SAML Server Instance \(NSM Procedure\) on page 188](#)
- [Configuring a Secure Access Active Directory or NT Domain Instance \(NSM Procedure\) on page 190](#)
- [Configuring a Secure Access eTrust SiteMinder Server Instance \(NSM Procedure\) on page 174](#)

Configuring a Secure Access Manual CA Certificate (NSM Procedure)

To manually upload CA certificates to the Secure Access device:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to manually upload CA certificates.
2. Click the **Configuration** tab, and then select **System > Configuration > Certificates > Trusted Client CAs** tab.
3. Click **Trusted Client CA**. The New Trusted Client CA page appears.
4. Configure the server using the settings described in [Table 47 on page 186](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 47: Secure Access Manual CA Certificate Configuration Details

Option	Function	Your Action
Settings tab		
Subject	Specifies the CA certificate subject name.	Enter a subject name for the certificate.
Client certificate status checking	Specifies the method the device uses to verify client certificate status.	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • None — Specifies that the device should not validate this trusted client certificate. • Use OCSP (Online Certificate Status Protocol) — Specifies that the device should use the OCSP method, validating the client certificate in real-time, as needed. After you select this option, you can specify options for OCSP. • Use CRLs (Certificate Revocation Lists)— Specifies that the device should use CRLs to validate the client certificate. After you select this option, you can specify options for CRL. • Use OCSP with CRL fallback—Specifies that the device should use the OCSP validation method when possible, but attempt to validate client certificates using CRLs should the OCSP method fail (for example, if the link to the OCSP Responder fails). After you select this option, you can specify options for both CRL and OCSP.
Verify Trusted Client CA	Specifies if you want the device to validate the CRL from which the certificate is issued.	Select the check box.
Trusted for Client Authentication?	Specifies if you want the device to trust this certificate when authenticating client certificates.	<p>Select the check box.</p> <p>NOTE: If you added this certificate for nonauthentication purposes (such as for SAML signature verification or machine certificate validation), disable this option. This indicates that the device must not trust any client certificate issued by this CA.</p>

Table 47: Secure Access Manual CA Certificate Configuration Details (*continued*)

Option	Function	Your Action
Participate in Client Certificate Negotiation	Specifies if you want to have the CA participate in client certificate selection for authentication.	<p>Select the check box.</p> <p>NOTE: In client certificate authentication or restriction, the device sends a list of all trusted client CAs configured in the trusted client CA store with this flag enabled to the user's browser for user certificate selection. The browser prompts the client certificates whose issuer CA and/or root CA is in that list. This option allows you to control which client certificate(s) are prompted for selection. Clearing this option for all certificates in a CA chain results in those certificates not being prompted.</p>
Import from	Specifies the trusted client file that you can import from the database.	Use Browse to select and import the trusted client files from.
OCSP > Settings tab		
OCSP settings	Specifies the OCSP method that the device uses to verify client certificate status.	<p>Select a value from the drop-down list. The list includes:</p> <ul style="list-style-type: none"> • Responder specified in CA certificate • Manually configured responders • Responder specified in Client certificate
Device Certificate to sign the request	Specifies the device certificate that is used to sign for the request.	Select a value from the drop-down list.
Use Nonce	Specifies the device to use nonce.	Select the check box to enable this option.
CRL Settings tab		
CDP(s) specified in the Trusted Client CA	Specifies the CDP(s) in the trusted client CA.	Select the check box to enable this option.
CDP(s) specified in the client certificate	Specifies the CDP(s) in the client certificate.	Select the check box to enable this option.
Manual configured CDP	Specifies the manual configured CDPs.	Select the check box to enable this option.
CRL Download Frequency (minutes)	Specifies the frequency of the CRL download.	Select the frequency of the CRL download. The default value is 1440.

- Related Documentation**
- [Configuring a Secure Access Certificate Server Instance \(NSM Procedure\) on page 184](#)
 - [Configuring a Secure Access SAML Server Instance \(NSM Procedure\) on page 188](#)

Configuring a Secure Access SAML Server Instance (NSM Procedure)

The Secure Access device accepts authentication assertions generated by an SAML authority using either an artifact profile or a POST profile. This feature allows a user to sign in to a source site or portal without going through the Secure Access device first, and then to access the Secure Access device with single sign-on (SSO) through the SAML consumer service.

To configure a new SAML server instance:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure an SAML server instance.
3. Click the **Configuration** tab and select **Authentication > Auth Servers**. The corresponding workspace appears.



NOTE: If you want to update an existing server instance, click the appropriate link in the Auth Server Name box, and perform the Steps 5 through 8.

4. Click the **New** button. The New dialog box appears.
5. In the Auth Server Name list, specify a name to identify the server instance.
6. Select **SAML Server** from the Auth Server Type list.
7. Configure the server using the settings described in [Table 48 on page 188](#).
8. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 48: SAML Server Instance Configuration Details

Option	Function	Your Action
SAML Settings > Basic Settings tab		
Source Site Inter-Site Transfer Service URL	Specifies the source site inter-site transfer service URL.	Enter the URL.
Issuer Value for Source Site	Specifies the issuer value for the source site.	Enter the URL or hostname of the issuer of the assertion.

Table 48: SAML Server Instance Configuration Details (*continued*)

Option	Function	Your Action
User Name Template	Specifies the user name template, which is a mapping string from the SAML assertion to a Secure Access user realm.	Enter the string.
Allow Clock Skew (minutes)	Determines the maximum allowed difference in time between the Secure Access device clock and the source site clock.	Enter the allowed clock skew value.
SAML Settings > Artifact SSO tab		
Source ID	Specifies the 20- byte identifier that the Secure Access device uses to recognize an assertion from a given source site.	Enter the Source ID.
Source SOAP Responder Service URL	Specifies the source SOAP responder service URL.	Enter a URL. NOTE: You should specify this URL in the form of an HTTPS: protocol.
SOAP Client Authentication	Specifies the SOAP client authentication.	Select either HTTP Basic or SSL Client Certificate .
Username	Specifies the username for SOAP client authentication.	Enter the username.
Password	Specifies password for SOAP client authentication.	Enter the password.
Device Certificate	Specifies the device certificate.	Select a device certificate the drop-down list.
SAML Settings > POST SSO tab		
Response Signing Certificate	Specifies the response signing certificate for the SAML response signature verification. This is the PEM-formatted signing certificate, which is loaded for the SAML response signature verification. The certificate you select should be the same certificate used for signing the SAML response at the source site. The source site may send this certificate along with the SAML response, depending on the source site configuration. By default, the system performs signature verification of the SAML response first on the locally configured certificate. If a certificate is not configured locally in the SAML authentication server, then the system performs the signature verification on the certificate included in the SAML response from the source site.	Enter the name or browse to locate the response signing certificate.
Issued To	Displays name and attributes of the entity to whom the certificate is issued.	Issued To details is displayed.

Table 48: SAML Server Instance Configuration Details (*continued*)

Option	Function	Your Action
Issued By	Displays name and attributes of the entity that issued the certificate.	Issued By details is displayed.
Valid	Displays the time range that the certificate is valid.	Certificate valid time range is displayed.
Enable Signing Certificate status checking	Allows the Secure Access device to check the validity of the signing certificate configured in the SAML authentication server POST profile.	Select SAML Settings > POST SSO > Enable Signing Certificate status checking to enable this feature.
Server Catalog > Expressions tab		
Name	Specifies a name for the user expression in the Certificate server user directory.	Enter the name.
Value	Specifies a value for the user expression in the Certificate server user directory.	Enter the value.

Related Documentation

- [Configuring a Secure Access Active Directory or NT Domain Instance \(NSM Procedure\) on page 190](#)
- [Configuring a Secure Access NIS Server Instance \(NSM Procedure\) on page 193](#)
- [Configuring a Secure Access Certificate Server Instance \(NSM Procedure\) on page 184](#)

Configuring a Secure Access Active Directory or NT Domain Instance (NSM Procedure)

To configure an Active Directory or Windows NT domain server instance:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure an Active Directory or NT domain instance.
3. Click the **Configuration** tab and select **Authentication > Auth Servers**. The corresponding workspace appears.



NOTE: If you want to update an existing server instance, click the appropriate link in the Auth Server Name box, and perform the steps 5 through 8.

4. Click the **New** button. The New dialog box appears.
5. In the Auth Server Name list, specify a name to identify the server instance.
6. Select **AD/NT Server** from the Auth Server Type list.

7. Configure the server using the settings described in [Table 49 on page 191](#).
8. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 49: Active Directory or NT Domain Instance Configuration Details

Option	Function	Your Action
AD/NT Settings > General tab		
Primary Domain Controller or Active Directory	Specifies the name or IP address for the primary domain controller or Active Directory server.	Enter the name or IP address.
Secondary Domain Controller or Active Directory	Specifies the name or IP address for the backup domain controller or Active Directory server.	Enter the name or IP address.
Domain	Specifies the domain name of the Active Directory or Windows NT server.	Enter the domain name of the Active Directory or Windows NT domain. NOTE: For example, if the Active Directory domain name is <code>us.amr.asgqa.net</code> and you want to authenticate users who belong to the US domain, enter US as the domain.
Allow domain to be specified as part of username	Allows users to sign in by entering a domain name in the Username box in the format: domain\username	Select AD/NT Settings > General > Allow domain to be specified as part of username to enable this feature.
Allow trusted domains	Allows users to get group information from all trusted domains within a forest.	Select AD/NT Settings > General > Allow trusted domains to enable this feature.
Domain Controller is a Windows 2008 server	Specifies if the backend domain controller is a Windows 2008 server. TIP: The Windows 2008 server has several enhancements to the Active Directory server, which is now called Active Directory Domain Services.	Select Domain Controller is a Windows 2008 server to enable this feature.
Admin Username	Specifies an administrator username for the AD or NT server.	Enter an administrator username for the AD or NT server.
Admin Password	Specifies an administrator password for the AD or NT server.	Enter an administrator password for the AD or NT server.
Kerberos (most secure)	Allows the Secure Access device to send user credentials to Kerberos.	Select AD/NT Settings > General > Kerberos (most secure) to enable this feature.

Table 49: Active Directory or NT Domain Instance Configuration Details (*continued*)

Option	Function	Your Action
NTLMV2 (moderately secure)	Allows the Secure Access device to send user credentials to NTLMv2.	Select AD/NT Settings > General > NTLMV2 (moderately secure) to enable this feature.
NTLMV1 (least secure)	Allows the Secure Access device to send user credentials to NTLMv1.	Select AD/NT Settings > General > NTLMV1 (least secure) to enable this feature.
Use LDAP to get Kerberos realm name	Allows the Secure Access device to retrieve the Kerberos realm name from the Active Directory server using the specified administrator credentials.	Select AD/NT Settings > General > Specify Kerberos realm name to enable this feature.
Specify Kerberos realm name	Specifies Kerberos realm name.	Enter the name.
AD/NT Settings > Advanced tab		
User may belong to Domain Local Groups across trust boundaries	Specifies that the selected user belongs to the Domain Local Groups who honor trust relationships in the Active Directory.	Select AD/NT Settings > Advanced > User may belong to Domain Local Groups across trust boundaries to enable this feature.
Container Name	Specifies the name that the Secure Access device uses to join the specified Active Directory domain as a computer.	Enter the computer name.
Server Catalog > Expressions tab		
Name	Specifies a name for the user expression in the Active Directory or NT domain server user directory.	Enter a name.
Value	Specifies a value for the user expression in the Active Directory or NT Domain server user directory.	Enter a value.
Server Catalog > Groups tab		
Name	Specifies the name of the group	Enter a name.
Groups	Specifies the admin's domain local groups information.	Enter a name.
AD Group	Specifies the group that contains the administrators to enable centralized administration in an Active Directory domain.	Enter a name.

Related Documentation

- [Configuring a Secure Access NIS Server Instance \(NSM Procedure\) on page 193](#)

- [Configuring Secure Access Authentication Realms \(NSM Procedure\) on page 195](#)
- [Configuring a Secure Access SAML Server Instance \(NSM Procedure\) on page 188](#)

Configuring a Secure Access NIS Server Instance (NSM Procedure)

When authenticating users with a UNIX/NIS server, the Secure Access device verifies that the username and password entered through the sign-in page corresponds to a valid user ID and password pair in the NIS server.

To configure an NIS server instance:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure NIS server instance.
3. Click the **Configuration** tab and select **Authentication > Auth Servers**. The corresponding workspace appears.



NOTE: If you want to update an existing server instance, click the appropriate link in the Auth Server Name box and perform the Steps 5 through 8.

4. Click the **New** button. The New dialog box appears.
5. Specify a name to identify the server instance.
6. Select **NIS Server** from the Auth Server Type list.
7. Configure the server using the settings described in [Table 50 on page 193](#).
8. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 50: Secure Access NIS Server Instance Configuration Details

Option	Function	Your Action
NIS Settings		
NIS Server	Specifies the name or IP address of the NIS server.	Enter the name or IP address.
NIS Domain	Specifies the domain name for the NIS server.	Enter the domain name.
Server Catalog > Expressions tab		
Name	Specifies a name for the user expression in the NIS server user directory.	Enter a name.

Table 50: Secure Access NIS Server Instance Configuration Details (*continued*)

Option	Function	Your Action
Value	Specifies a value for the user expression in the NIS server user directory.	Enter a value.

Related Documentation

- [Configuring Secure Access Authentication Realms \(NSM Procedure\) on page 195](#)
- [Configuring Secure Access Authentication Policies \(NSM Procedure\) on page 198](#)
- [Configuring a Secure Access Active Directory or NT Domain Instance \(NSM Procedure\) on page 190](#)

Configuring Authentication Realms

- [Configuring Secure Access Authentication Realms \(NSM Procedure\) on page 195](#)
- [Configuring Secure Access Authentication Policies \(NSM Procedure\) on page 198](#)
- [Configuring Secure Access Role Mapping Rules \(NSM Procedure\) on page 203](#)

Configuring Secure Access Authentication Realms (NSM Procedure)

An authentication realm specifies the conditions that users must meet to sign into the Secure Access device.

To configure an authentication realm:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure authentication realms.
2. Click the **Configuration** tab, select **Administrators > Admin Realms** or **Users > User Realms**. The corresponding workspace appears.
3. Click the **New** button. The New dialog box appears.
4. Configure the server using the settings described in [Table 51 on page 195](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 51: Secure Access Authentication Realms Configuration Details

Option	Function	Your Action
General tab		
Realm Name	Specifies the name of the realm.	Enter a name.
Description	Describes the realm.	Enter a description.
When editing, start on the Role Mapping page	Specifies that the Role Mapping tab is selected when you open the realm for editing.	Select General > When editing, start on the Role Mapping page to enable this option.

Table 51: Secure Access Authentication Realms Configuration Details (*continued*)

Option	Function	Your Action
Authentication	Specifies an authentication server to use for authenticating users who sign in to this realm.	Select an authentication server from the drop-down list.
Directory/Attribute	Specifies a directory/attribute server to use for retrieving user attribute and group information for role mapping rules and resource policies.	Select a directory/attribute server from the drop-down list (optional).
Accounting	Specifies a RADIUS accounting server to use to track when a user signs in and out of the Secure Access device.	Select a RADIUS accounting server from the drop-down list (optional).
Additional Authentication Server	Specifies the name of the secondary authentication server to submit secondary user credentials to an SSO-enabled resource or enable two-factor authentication to access the Secure Access device. NOTE: You cannot choose an anonymous server, certificate server, or eTrust SiteMinder server.	Select a secondary authentication server from the drop-down list.
End session if authentication against this server fails	Controls access to the Secure Access device based on the successful authentication of the user's secondary credentials. If selected, authentication fails if the user's secondary credentials fail.	Select General > End session if authentication against this server fails to enable this option.
Username for Secondary Auth	Specifies the username of the secondary authentication server.	Select the mode of submission of username to the secondary authentication server from the drop-down list: <ul style="list-style-type: none"> Username is specified by user on sign-in page—Prompts the user to manually submit his username to the secondary server during the Secure Access device sign-in process. Predefined user name template—Automatically submits a username to the secondary server during the Secure Access device sign-in process.
Predefined User Name	Specifies the predefined username.	Enter static text or a valid variable.

Table 51: Secure Access Authentication Realms Configuration Details (*continued*)

Option	Function	Your Action
Password for Secondary Auth	Specifies the password for the secondary authentication server.	<p>Select the mode of submission of password to the secondary authentication server from the drop-down list:</p> <ul style="list-style-type: none"> • Username is specified by user on sign-in page—Prompts the user to manually submit his password to the secondary server during the Secure Access device sign-in process. • Predefined user name template—Automatically submits a password to the secondary server during the Secure Access device sign-in process.
Predefined Password	Specifies the predefined password.	Enter static text or a valid variable.
Enable Dynamic policy evaluation	Uses dynamic policy evaluation for this realm.	Select General > Enable Dynamic policy evaluation to enable an automatic timer for dynamic policy evaluation of this realm's authentication policy, role mapping rules, and role restrictions.
Refresh roles	Refreshes the roles of all users in this realm. (This option does not control the scope of the Refresh Now button.)	Select General > Refresh roles to enable this option.
Refresh policies	Refreshes the resource policies (not including Meeting and Email Client) for all users in this realm. (This option does not control the scope of the Refresh Now button.)	Select General > Refresh policies to enable this option.
Refresh interval (minutes)	Specifies how often you want the Secure Access device to perform an automatic policy evaluation of all currently signed-in realm users.	Enter the number of minutes (5 to 1440).

Related Documentation

- [Configuring Secure Access Authentication Policies \(NSM Procedure\) on page 198](#)
- [Configuring Secure Access Role Mapping Rules \(NSM Procedure\) on page 203](#)
- [Configuring Secure Access Sign-In Policies \(NSM Procedure\) on page 207](#)

Configuring Secure Access Authentication Policies (NSM Procedure)

An authentication policy is a set of rules that controls one aspect of access management—whether or not to present a realm’s sign-in page to a user. An authentication policy is part of an authentication realm’s configuration, specifying rules for the Secure Access device to consider before presenting a sign-in page to a user.

To configure an authentication realm policy:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure an authentication realm policy.
2. Click the **Configuration** tab, and then select **Administrators > Admin Realms** or **User or Users Realms**. The corresponding workspace appears.
3. Click the **New** button. The New dialog box appears.
4. Configure the server using the settings described in [Table 52 on page 198](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 52: Authentication Realm Policies Configuration Details

Option	Function	Your Action
Authentication Policies > Source IP tab		
Allow	Controls from which IP addresses users can access a Secure Access device sign-in page, be mapped to a role, or access a resource.	<p>Select any one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • Users from any IP address—Enables users to sign into the Secure Access device from any IP address to satisfy the access management requirement. • User from IP addresses which pass the specified matching policies—Enables users to sign into the Secure Access device from IP addresses that have passed the specified matching policies.
Source IP Address	Specifies the IP address of the sender.	<p>Enter the IP address.</p> <p>NOTE: The new button is enabled only when you select User from IP addresses which pass the specified matching policies option from the Allow drop-down list.</p>
Source IP Netmask	Specifies the IP Netmask.	<p>Enter the IP netmask.</p> <p>NOTE: The new button is enabled only when you select Allow or deny users from the following IP addresses option from the Allow drop-down list.</p>

Table 52: Authentication Realm Policies Configuration Details (*continued*)

Option	Function	Your Action
Access	Allows or denies users to sign in from the specified IP address.	<p>Select one of the following options from the drop-down list:</p> <p>Allow—Allows users to sign in from the specified IP address.</p> <p>Deny—Prevents users from signing in from the specified IP address.</p>
Authentication Policies > Browser tab		
Allow	Controls from which Web browsers users/admins can access the sign-in page of the Secure Access device, be mapped to a role, or access a resource. You are prompted with a sign-in attempt failed error message when you try to sign in to the device using an unsupported browser.	<p>Select one of the following options from the drop-down list:</p> <p>Browsers with any user-agent—Allows you to sign into the device from any browser and the device submits the user credentials to the authentication server.</p> <p>Browsers whose user-agents pass the matching policies defined below—Allows you to sign in from a browser whose user-agent string meets the specified pattern requirements for the selected authentication realm.</p>
User agent pattern	Specifies the user agent pattern.	<p>Enter a string in the format <code>*<browser_string>*</code></p> <p>NOTE: This option is enabled only when you select Browsers whose user-agents pass the matching policies defined below from the Allow drop-down list and then by clicking New.</p>
Action	Allows or denies users to use a browser that has a user-agent header containing the <code><browser-string>substring</code> .	<p>Select one of the following options from the drop-down list:</p> <p>Allow—Allows users to use a browser that has a user-agent header containing the <code><browser_string></code> substring.</p> <p>Deny—Prevents users from using a browser that has a user-agent header containing the <code><browser_string></code> substring.</p> <p>NOTE: This option is enabled only when you select Browsers whose user-agents pass the matching policies defined below from the Allow drop-down list and then by clicking New.</p>
Authentication Policies > Certificate tab		

Table 52: Authentication Realm Policies Configuration Details (*continued*)

Option	Function	Your Action
Allow	Restricts the Secure Access device and resource access by requiring client-side certificates.	<p>Select one of the following options from the drop-down list:</p> <p>All users—Does not require a user's client to have a client-side certificate.</p> <p>All users, remember certificate while user is signed in—Does not require a user's client to have a client-side certificate, but if the client does have a certificate, the Secure Access device remembers the certificate information during the entire user session.</p> <p>Users with a trusted client certificate—Requires a user's client to have a client-side certificate to satisfy the access management requirement. To restrict access even further, you can define unique certificate attribute-value pairs. Note that the user's certificate must have all the attributes you define.</p>
Certificate Field	Specifies any additional criteria that the admin realm should use when verifying the policies.	<p>Enter a value. For example, enter uid.</p> <p>NOTE: This field is enabled only when you select Users with trusted client certificate from the Allow drop-down list and by clicking New.</p>
Expected Value	Specifies values in the client certificate.	<p>Enter a variable, for example, enter <userAttr.uid>.</p> <p>NOTE: This field is enabled only when you select Users with trusted client certificate from the Allow drop-down list and by clicking New.</p>
Authentication Policies > Password tab		
Options for primary authentication server	Restricts the Secure Access device and resource access by password length when administrators or users try to sign in to a Secure Access device. The user must enter a password whose length meets the minimum password-length requirement specified for the realm.	<p>Select one of the following options from drop-down list:</p> <p>Allow all users (passwords of any length)—Does not apply password length restrictions to users signing in to the Secure Access device.</p> <p>Only allow users that have passwords of a minimum length—Requires the user to enter a password with a minimum length of the number specified.</p>
Primary password minimum length (character)	Specifies password length restrictions.	Enter the number.

Table 52: Authentication Realm Policies Configuration Details (*continued*)

Option	Function	Your Action
Options for secondary authentication server	Restricts the Secure Access device and resource access by password-length to the secondary authentication server when administrators or users try to sign in to an Secure Access device. The user must enter a password whose length meets the minimum password-length requirement specified for the realm.	<p>Select one of the following options from the drop-down list:</p> <p>Allow all users (passwords of any length)—Does not apply password length restrictions to users signing in to the Secure Access device.</p> <p>Only allow users that have passwords of a minimum length—Requires the user to enter a password with a minimum length of the number specified.</p>
Secondary password minimum length (character)	Specifies password length restrictions.	Enter the number.
Authentication Policies > Host Checker tab		
Evaluate ALL policies	Evaluates all the policies without enforcing the policy on the client and allows user access.	Select Authentication Policies > Host Checker > Evaluate ALL policies to enable this feature.
Enforce ALL policies	Enforces all the policies on the client for the user to log in to the specified realm.	Select Authentication Policies > Host Checker > Enforce ALL policies to enable this feature.
Evaluate selected policies	Evaluates the selected policies without enforcing the policy on the client and allows user access.	Select the policy, and then click Add .
Enforce selected policies	Enforces the policies on the client for the user to log in to the specified realm.	Select a policy, and then click Add .
Evaluate logic	Does not require users to meet all of the requirements in all of the selected policies. Instead, the user can access the realm if he meets the requirements of any one of the selected Host Checker policies.	<p>Select one of the following options from the drop-down list:</p> <p>allow access to realm if any ONE of the selected Require & Enforce policies succeed—User can access the realm if he meets the requirements of any one of the selected Host Checker policies.</p> <p>Allow access only if all of the Require & Enforce policies succeed—User can access the realm only if he meets all of the requirements in all of the selected policies.</p>
Authentication Policies > Cache Cleaner tab		

Table 52: Authentication Realm Policies Configuration Details (*continued*)

Option	Function	Your Action
Cache Cleaner option	<p>Specifies the cache cleaner restrictions.</p> <p>NOTE: The Cache Cleaner tab is displayed only when you configure user realm policies.</p>	<p>Select one of the following option:</p> <p>Disable Cache Cleaner— Does not require Cache Cleaner to be installed or running for the user to meet the access requirement.</p> <p>Just load Cache Cleaner (Loads after IVE maps the user to a realm)—Does not require Cache Cleaner to be running for the user to meet the access requirement but ensures that it is available for future use. If you choose this option for a realm's authentication policy, then the Secure Access device downloads Cache Cleaner to the client machine after the user is authenticated and before the user is mapped to any roles on the system.</p> <p>Load and enforce Cache Cleaner (Loads before IVE maps the user to a realm)—Requires the Secure Access device to download and run Cache Cleaner for the user to meet the access requirement. If you choose this option for a realm's authentication policy, then the Secure Access device downloads Cache Cleaner to the client machine before the user may access the Secure Access device sign-in page.</p>
Authentication Policies > Limits tab		
Limit number of concurrent users	Limits the number of concurrent users on the realm.	Select Authentication Policies > Limits > Limit number of concurrent users to enable this feature.
Guaranteed minimum	Specifies any number of users between zero (0) and the maximum number of concurrent users defined for the realm, or you can set the number up to the maximum allowed by your license if there is no realm maximum.	Enter a number.
Maximum	Specifies any number of concurrent users from the minimum number you specified up to the maximum number of licensed users. If you enter a zero (0) into the Maximum box, no users are allowed to login to the realm.	Enter a number.

Related Documentation

- [Configuring Secure Access Role Mapping Rules \(NSM Procedure\) on page 203](#)
- [Configuring Secure Access Sign-In Policies \(NSM Procedure\) on page 207](#)

- [Configuring Secure Access Authentication Realms \(NSM Procedure\) on page 195](#)

Configuring Secure Access Role Mapping Rules (NSM Procedure)

Role mapping rules are conditions a user must meet for the device to map the user to one or more user roles. These conditions are based on either user information returned by the realm's directory server or the user's username.

To configure role mapping rules for an administrator/user realm:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure role mapping rules for an administrator/user realm.
3. Click the **Configuration** tab and select either **Administrators > Admin Realms** or **Users > User Realms**. The corresponding workspace appears.
4. Click the **New** button. The New dialog box appears.
5. Configure role mapping rules for an administrator/user realm using the settings described in [Table 53 on page 203](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 53: Role Mapping Rules Configuration Details

Option	Function	Your Action
Role Mapping Rules tab		
User must select from among assigned roles	Specifies if you want the users to select from the assigned roles.	Select Admin Realm > Role Mapping Rules > User must select from among assigned roles to enable this option.
User must select the sets of merged roles assigned by each rule	Specifies if you want users to select the sets of merged roles that are assigned by each rule.	Select Admin Realm > Role Mapping Rules > User must select the sets of merged roles assigned by each rule to enable this option.
Role Mapping Rules > New > Settings tab		
Name	Specifies the name entered on the sign-in page.	Enter a name.
Assign these roles if the rule matches >Non-members	Specifies the list of non-members whose roles are not matched with the rules.	Select a non-member from the list to assign to the authenticated user by adding/removing it to/from the Members list.

Table 53: Role Mapping Rules Configuration Details (*continued*)

Option	Function	Your Action
Stop processing rules when this rule matches	Specifies if you want the device to stop evaluating role mapping rules if the user meets the conditions specified for this rule.	Select Admin Realms > Role Mapping Rules > Settings > Stop processing rules when this rule matches to enable this option.
Role mapping rule type	Specifies the type of role mapping rule.	<ul style="list-style-type: none"> Select If user name if the role mapping parameter must be based on the user name. Select is/is not conditional expressions for the rule, click the Add button, and enter the new user names. Select If certificate has any of the attributes if the role mapping parameter must be based on the certificate attributes. Select is/is not conditional expressions for the rule, click the Add button, and enter the new values. Select If user has any of these custom expressions if the role mapping parameter must be based on the custom expressions. The collection-of-expressions button appears. <ol style="list-style-type: none"> Click the collection-of-expressions button to assign expressions. The expressions that were created for the selected authentication server appears. Select an existing expression from the Non-members area and click Add to assign the expression to the role-mapping rule. Click New and create an expression to assign a new expression to the role-mapping rule. For information on creating custom expressions and using the Expression Dictionary, refer to "Creating a Custom Expression for an Authentication Server (NSM Procedure)." <p>NOTE: You can create a custom expression in a device template, but you cannot validate the custom expression. The Validate button is not enabled in the Custom Expressions editor for device templates.</p>
is/is not NOTE: This option is enabled only if you select either if username or if certificate has any of the attributes as the role mapping rule type.	Specifies the conditional expression used in the rule.	Select an option from the drop-down list.

Table 53: Role Mapping Rules Configuration Details (*continued*)

Option	Function	Your Action
New	Specifies the rules that are used for matching.	Enter the respective rule matching entries. NOTE: <ul style="list-style-type: none"> Enter a new username if you select if username as role mapping rule type. Enter a new expression if you select if user has any of these custom expressions as role mapping rule type. Enter a new value if you select if certificate has any of the attributes as role mapping rule type.
Attribute	Specifies the role mapping role attributes. NOTE: This option is enabled only if you select if certificate has any of the attributes as the role mapping rule type.	Enter an attribute name.

- Related Documentation**
- [Configuring Secure Access Sign-In Policies \(NSM Procedure\) on page 207](#)
 - [Configuring Secure Access Authentication Policies \(NSM Procedure\) on page 198](#)

Configuring Sign-in Policies and Sign-in Pages

- [Configuring Secure Access Sign-In Policies \(NSM Procedure\) on page 207](#)
- [Configuring Secure Access Sign-In Pages \(NSM Procedure\) on page 211](#)

Configuring Secure Access Sign-In Policies (NSM Procedure)

You can create sign-in policies to define URLs that you can use to access the Secure Access device. There are two types of sign-in policies—one for users and one for administrators. When configuring sign-in policies, you must associate realms, sign-in pages, and URLs.

To configure sign-in policies, you must follow these procedures:

1. [Creating Authorization-Only Policies on page 207](#)
2. [Creating User or Administrator URLs on page 209](#)
3. [Creating Meeting URLs on page 210](#)

Creating Authorization-Only Policies

The authorization-only policy is similar to a reverse proxy. Typically, a reverse proxy is a proxy server that is installed in front of the Web Servers.

With an authorization-only policy, you select a user role. The device acts as a reverse proxy server and performs authorization against the Netegrity SiteMinder server for each request.

To configure an authorization-only policy:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the Device Tree tab, and then double-click the Secure Access device for which you want to configure an authorization-only policy.
2. Click the **Configuration** tab, and select **Authentication > Signing In > Sign-in Policies > Authorization-Only Policies**. The corresponding workspace appears.

3. Add or modify settings on the authorization-only policy as specified in [Table 54 on page 208](#).
4. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 54: Authorization-Only Policy Configuration Details

Option	Function	Your Action
Virtual Hostname	Accesses the backend application and sends the request to the original requesting Web browser.	Enter a valid name that maps to the device's IP address. NOTE: The name must be unique among all the virtual hostnames used in pass-through proxy's hostname mode. Also, do not include the protocol (for example, http:) in this option.
Backend URL	Allows the client to redirect to this URL. The request from the virtual hostname gets transformed as a request to this URL.	Enter a valid URL for the remote server. NOTE: You must specify the protocol, hostname, and port of the server. For example, enter <code>http://www.mydomain.com:8080/*</code> .
Description	Specifies the description of the policy.	Enter a description for the policy.
Authorization Server	Specifies the Netegrity SiteMinder server that manages user authentication and access.	Select the corresponding Netegrity SiteMinder server.
Role Option	Specifies the user role.	Select one of the user role options. NOTE: Only the following user role options are applicable for authorization-only policies. <ul style="list-style-type: none"> • Allow browsing un-trusted SSL (Users > User Roles > RoleName > Web > Options). • HTTP connection timeout (Users > User Roles > RoleName > Web > Options). • Source IP restrictions (Users > User Roles > RoleName > General > Restrictions). • Browser restrictions (Users > User Roles > RoleName > General > Restrictions).
Enable	Enables or disables the individual policy.	Select Authorization-Only Policies > Enable to enable this option.

Table 54: Authorization-Only Policy Configuration Details (*continued*)

Option	Function	Your Action
Allow ActiveSync Traffic only	Enables or disables only the ActiveSync requests.	Select Allow ActiveSync Traffic only to perform a basic validation of the HTTP header to ensure the request is consistent with the ActiveSync protocol. If you select this option, only ActiveSync protocol requests can be processed. If validation fails, a message is created in the user's event log. If you do not select this option, both ActiveSync and non-ActiveSync requests are processed.

Creating User or Administrator URLs

To configure a user or administrator URL:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the Device Tree tab, and then double-click the Secure Access device for which you want to configure a user/administrator URL.
2. Click the **Configuration** tab, and select **Authentication > Signing In > Sign-in Policies > User/Administrator URLs**. The corresponding workspace appears.
3. Add or modify settings on the user/administrator URL as specified in [Table 55 on page 209](#).
4. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 55: User/Administrator URLs Configuration Details

Option	Function	Your Action
General tab		
Sign-in URL	Specifies the sign-in URL.	Enter a valid URL for the sign-in URL.
Description	Specifies the description of the user/administrator URL policy.	Enter a description for the user/administrator URL policy.
Enable	Enables or disables the individual policy.	Select User/Administrator URLs > Enable to enable this option.
Sign-in Page	Specifies the customized properties in the end-user's welcome page such as the welcome text, help text, logo, header, and footer.	Select the sign-in page from the drop-down list.
Realm Select	Specifies the type of the realm that you want to choose.	Select the realm select from the drop-down list.

Table 55: User/Administrator URLs Configuration Details (*continued*)

Option	Function	Your Action
Administrator > Selected Admin Realms > Non-members	Moves the selected admin realms from non-members to members.	Select the admin realms from Non-members to Members.
User > Meeting URL	Specifies the URL that controls the sign-in page, which you can view when you sign into a meeting on the Secure Access device.	Select the meeting URL from the drop-down list.
User > Selected User Realms > Non-members	Moves the selected user realms from non-members to members.	Select the user realms from Non-members to Members.

Creating Meeting URLs

To configure a meeting URL:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the Device Tree tab, and then double-click the Secure Access device for which you want to configure a meeting URL.
2. Click the **Configuration** tab, and select **Authentication > Signing In > Sign-in Policies > Meeting URLs**. The corresponding workspace appears.
3. Add or modify settings on the meeting URL as specified in [Table 56 on page 210](#).
4. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 56: Meeting URLs Configuration Details

Option	Function	Your Action
User Type	Specifies the type of sign-in policy.	Select the type of policy from the drop-down list (for example, enter Meeting).
Sign-in URL	Specifies the URL that you want to associate with the meeting URL policy.	Enter a valid URL. NOTE: Use the format <host>/<path> where <host> is the hostname of the device and <path> is any string that you enter.
Description	Describes of the meeting URL policy.	Enter a description of the meeting URL policy.
Enable	Enables or disables the individual policy.	Select Meeting URLs > Enable to enable this option.

Table 56: Meeting URLs Configuration Details (*continued*)

Option	Function	Your Action
Sign-in Page	Specifies the meeting sign-in page.	Select a meeting sign-in page from the drop-down list.

- Related Documentation**
- [Configuring Secure Access Sign-In Pages \(NSM Procedure\) on page 211](#)
 - [Configuring a SAML Access Control Resource Policy \(NSM Procedure\) on page 223](#)

Configuring Secure Access Sign-In Pages (NSM Procedure)

A sign-in page defines the customized properties in the end-user's welcome page such as the welcome text, help text, logo, header, and footer. It also allows you to create two types of sign-in pages to present to users and administrators such as standard and customized sign-in pages.

To configure sign-in policies, you must follow these procedures:

1. [Creating Users/Administrator Sign-in Pages on page 211](#)
2. [Creating Meeting Sign-in Pages on page 213](#)

Creating Users/Administrator Sign-in Pages

To configure a user or administrator sign-in page:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the Device Tree tab, and then double-click the Secure Access device for which you want to configure a user/administrator sign-in page.
2. Click the **Configuration** tab, and select **Authentication > Signing In > Sign-in Pages > Users/Administrator Sign-in Pages**. The corresponding workspace appears.
3. Add or modify settings on the user/administrator sign-in page as specified in [Table 57 on page 211](#).
4. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 57: Users/Administrator Sign-in Pages Configuration Details

Option	Function	Your Action
Settings tab		
Name	Specifies the name of the user or administrator sign-in page.	Enter a name for the user or administrator sign-in page.
Sign-in Page Type	Specifies the type of sign-in page.	Select any sign-in page type such as Standard or Custom Sign-In Pages .
Settings > Sign-in Page Type > Standard > Custom Text tab		

Table 57: Users/Administrator Sign-in Pages Configuration Details (continued)

Option	Function	Your Action
Welcome message	Specifies the welcome message for the sign-in page.	Enter or update the default welcome message for the sign-in page.
Portal Name	Specifies the portal name of the sign-in page.	Enter a portal name for the sign-in page.
Submit button	Specifies the name of the command button that you would like to show in the sign-in page.	Enter an appropriate name for the button. For example, enter Sign In .
Instructions	Specifies the instructions that you may want to know while signing in.	Enter an appropriate message for the user to perform while signing in. For example, enter Please sign in to begin your secure session .
Username	Specifies the username of the sign-in page.	Enter your username.
Password	Specifies the password of the respective username that you enter.	Enter a valid password for the username you have entered.
Realm	Specifies the realm of the sign-in page.	Enter the realm name.
Secondary username	Specifies the alternate or the secondary username.	Enter the alternate or the secondary username.
Secondary password	Specifies the password for the secondary username.	Enter the password for the secondary username.
Prompt the secondary credentials on the second page	Prompts the user that the secondary credentials are displayed in the second page.	Select Custom Text > Prompt the secondary credentials in the second page to enable this option.
Sign Out message	Specifies the sign-out message that the user needs to be informed of.	Enter an appropriate message for the user while performing a sign out. For example, enter Your session has ended .
Sign In link text	Specifies the link if the user must be prompted to sign in again.	Click the respective link to sign in again.
Settings > Sign-in Page Type > Standard > Header Appearance tab		
Logo image	Specifies the custom logo image file for the header.	Select the image file using the browse button.
Background color	Specifies the background color for the header.	Select any background color using the color palette.

Table 57: Users/Administrator Sign-in Pages Configuration Details (continued)

Option	Function	Your Action
Settings > Sign-in Page Type > Standard > Custom Error Messages tab		
Missing certificate	Prompts you that there is some missing certificate information.	Enter an appropriate error message for the missing certificate. For example, enter Missing certificate. Check that your certificate is valid and up-to-date, and try again.
Invalid certificate	Prompts you that the selected certificate is an invalid or expired certificate.	Enter an appropriate error message for the invalid certificate. For example, enter Invalid or expired certificate. Check that your certificate is valid and up-to-date, and try again.
Settings > Sign-in Page Type > Standard > Help tab		
Show Help Button	Prompts the user that there is Help available in the sign-in page.	Select Help > Show Help Button to enable this option.
Help	Specifies the name of the Help button to be shown on the page.	Enter an appropriate name for the Help button. For example, enter Help .
HTML File	Allows the administrator to select the HTML file that needs to be displayed when the user clicks the Help button on the page.	Select the respective Help file from its location using the browse button.
Settings > Sign-in Page Type > Custom Sign-In Pages		
Templates File	Specifies the template file.	Select a template file from the drop-down list or use the browse button.
Current Templates File	Specifies the current template file.	Automatically displays the current template file and it is not editable.
File Upload Time	Specifies the time taken to upload the template file.	Automatically displays the file upload time and it is not editable.

Creating Meeting Sign-in Pages

To configure a meeting sign-in page:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the Device Tree tab, and then double-click the Secure Access device for which you want to configure a meeting sign-in pages.
2. Click the **Configuration** tab, select **Authentication > Signing In > Sign-in Policies > Meeting Sign-in Pages**. The corresponding workspace appears.
3. Add or modify settings on the meeting sign-in page as specified in [Table 58 on page 214](#).
4. Click one:

- **OK**—Saves the changes.
- **Cancel**—Cancels the modifications.

Table 58: Meeting Sign-in Page Configuration Details

Option	Function	Your Action
Settings tab		
Name	Specifies the name of the secure meeting sign-in page.	Enter a name for the secure meeting sign-in page.
Sign-in Page Type	Specifies the type of the sign-in page.	Select any sign-in page type such as Standard or Custom Sign-In Page .
Settings > Sign-in Page Type > Standard > Custom Text tab		
Welcome message	Specifies the welcome message for the secure meeting sign-in page.	Enter or update the default welcome message for the secure meeting sign-in page.
Portal Name	Specifies the portal name of the secure meeting sign-in page.	Enter a portal name for the secure meeting sign-in page.
Submit button	Specifies the name of the command button that you would like to show in the secure meeting sign-in page.	Enter an appropriate name for the button. For example, enter Sign In .
Instructions	Specifies the instructions that you may want the user to know while signing in.	Enter an appropriate message for the user to perform while signing in for the secure meeting. For example, enter Please sign in to begin your secure session .
Meeting ID	Specifies the meeting ID of the secure meeting.	Enter a meeting ID for the secure meeting.
Your Name	Specifies the name of the meeting organizer.	Enter your username.
Meeting Password	Specifies the password for the secure meeting.	Enter the password for the secure meeting.
Logo image	Specifies the custom logo image file for the header.	Select the image file using the browse button.
Background color	Specifies the background color for the header.	Select any background color using the color palette.
Settings > Sign-in Page Type > Custom Sign-In Page		
Templates File	Specifies the template file.	Select a template file from the drop-down list or use the browse button.

Table 58: Meeting Sign-in Page Configuration Details (*continued*)

Option	Function	Your Action
Current Templates File	Specifies the current template file.	Automatically displays the current template file and it is not editable.
File Upload Time	Specifies the time taken to upload the template file.	Automatically displays the file upload time and it is not editable.

Related Documentation

- [Configuring a SAML Access Control Resource Policy \(NSM Procedure\) on page 223](#)
- [Configuring Secure Access Sign-In Policies \(NSM Procedure\) on page 207](#)

CHAPTER 14

Configuring Single Sign-On

- [Defining Basic, NTLM, and Kerberos Resources on page 217](#)
- [Configuring Basic, NTLM, and Kerberos Resources \(NSM Procedure\) on page 218](#)
- [Defining a Basic Authentication, NTLM, or Kerberos Intermediation Resource Policy \(NSM Procedure\) on page 221](#)
- [Configuring a SAML Access Control Resource Policy \(NSM Procedure\) on page 223](#)
- [Configuring SAML SSO Artifact Profile Resource Policy \(NSM Procedure\) on page 226](#)

Defining Basic, NTLM, and Kerberos Resources

You can set up basic, NT LAN Manager (NTLM), and Kerberos credentials in the Devices > Users > Resource Policies > Web > SSO > General tab. Follow these guidelines when managing single sign-on (SSO):

- The Secure Access device manages Kerberos if challenged with the negotiate header, NTLM if challenged with the NTLM header; and basic authentication if challenged with the basic resource.
- If the device receives multiple challenges, the order of precedence is as follows:
 - Kerberos
 - NTLM
 - Basic
- The device first sets the constrained delegation if the service is configured in a service list.
- Policy configurations override any settings in the SSO > General tab.
- Disabling all the options available in the SSO > General screen prevents SSO. However, the device continues to an intermediate phase and displays an intermediation page to the enduser.
- You can explicitly turn off the basic authentication intermediation in a policy. For Kerberos and NTLM, the device will always be intermediate.
- Depending on the SSO used, you can view the different fields in the intermediation page and configure the following options:
 - Basic authentication intermediation page—Displays username and password fields.

- NTLM intermediation page—Displays username, password, and domain fields.
- Kerberos intermediation page—Displays username, password, and realm fields.
- When upgrading a Secure Access device or performing a new installation, the default SSO BasicAuthNoSSO policy is preserved. If you have enabled all options of the General tab, SSO will not be enabled until you have deleted the BasicAuthNoSSO policy.

Related Documentation

- [Configuring Basic, NTLM, and Kerberos Resources \(NSM Procedure\) on page 218](#)
- [Defining a Basic Authentication, NTLM, or Kerberos Intermediation Resource Policy \(NSM Procedure\) on page 221](#)
- [Configuring a SAML Access Control Resource Policy \(NSM Procedure\) on page 223](#)

Configuring Basic, NTLM, and Kerberos Resources (NSM Procedure)

To configure basic, NT LAN Manager (NTLM), and Kerberos resources:

1. In the navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure the basic, NTLM, and Kerberos resources.
3. Click the **Configuration** tab. Select **Users > Resource Policies > Web > General**.
4. Click the **New** icon to configure the options as described in [Table 59 on page 218](#).
5. Click **OK** to save the changes.

Table 59: Configuring Basic, NTLM, and Kerberos Resources

Options	Your Action
General > Kerberos tab	
Enable Kerberos SSO	Select the Enable Kerberos SSO check box to enable Kerberos SSO.
General > Kerberos > Realm Definition > New Realm Definition	
Realm	Enter the Kerberos realm name. For example, enter http://www.kerber.net . The device uses kerber.net to obtain the list of key distribution centers (KDCs).
Site Name	Enter the Active Directory site names. Use this field to have the device contact the KDC at a specific site. For example, if site name is Sunnyvale and realm is http://www.kerber.net, then the device uses Sunnyvale.KERBER.NET to get the list of KDCs. NOTE: The Active Directory must have the sites defined and DNS must be configured to return the KDCs in the site.
Pattern	Enter the hostnames mapped to the Kerberos realm. You can enter wildcard characters such as *.y.com, *.kerber.net, or *.*

Table 59: Configuring Basic, NTLM, and Kerberos Resources (*continued*)

Options	Your Action
KDC	Enter the hostname or IP address of the KDCs if DNS is unavailable or if you want the device to contact a specific KDC for tickets. If you enter a KDC, the device does not use DNS to obtain the list of KDCs based on the values entered in the Site Name and Realm boxes.
General > Kerberos > Constrained Delegation > Constrained Delegation > New Constrained Delegation	
Label	Enter a name to uniquely identify the constrained delegation. No external mapping is made to the label value.
Realm	Select the realm to use. The drop-down list is populated by values in the Realm box.
Principal Account	Enter the constrained delegation account. The device obtains the constrained delegation tickets with the value you enter on behalf of the user.
Password	Enter the constrained delegation account password.
Service List	Select the service list to use. The list should be an exact match with the service list in Active Directory if you want the device to perform constrained delegation for all the services. Hostnames must be an exact match.
General > Kerberos > Constrained Delegation > Constrained Delegation Services List > New Constrained Delegation Service List	
Id	Enter a unique identification number for the constrained delegation service list.
Name	Enter a name for the constrained delegation service list.
Services	Enter the service list name.
General > Kerberos > Kerberos Intermediation > Kerberos Intermediation > New Kerberos Intermediation	
Label	Enter a name to uniquely identify the Kerberos Intermediation. No external mapping is made to the label value.
Realm	Select the realm to use. The drop-down list is populated by values in the Realm box.
Credential Type	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • System—Specifies the set of user credentials, such as primary and secondary authorization credentials, stored in the device. If you select this option, you do not need to enter the username and password. • Variable—Allows tokens such as username and password to be used in the Username and Password boxes. • Static—Specifies the username and password exactly as they are entered in the Username and Password boxes.
Username	Enter the account username.
Password	Enter the account password.
Variable Password	Enter the password token if you select Variable as the credential type.

Table 59: Configuring Basic, NTLM, and Kerberos Resources (*continued*)

Options	Your Action
General > NTLM	
Enable NTLM SSO	Select the Enable NTLM SSO check box to enable NTLM SSO. If you do not enter any configuration information, the device attempts to figure out the domain from the hostname and performs SSO using the system credentials.
Fallback to NTLM V1	Select the Fallback to NTLM V2 check box to fall back to NTLMv1 if Kerberos fails. If you do not select this option and Kerberos SSO fails, an intermediation page appears.
General > NTLM > NTLM Intermediation > New NTLM Intermediation	
Label	Enter a name to uniquely identify the NTLM intermediation. No external mapping is made to the label value.
domain	Enter the Active Directory domain name.
Credential Type	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • System—Specifies the set of user credentials, such as primary and secondary authorization credentials, stored in the device. If you select this option, you do not need to enter the username and password. • Variable—Allows tokens such as username and password to be used in the Username and Password boxes. • Static—Specifies the username and password exactly as they are entered in the Username and Password boxes.
Username	Enter the account username. If you select Variable as the credential type, you can enter the username token.
Password	Enter an account password.
Variable Password	Enter the password token if you select Variable as the credential type.
General > Basic Authentication	
Enable Basic Authentication SSO	Select the Enable Basic Authentication SSO check box to enable basic authentication SSO.
General > Basic Authentication > Basic Auth Intermediation > New Basic Auth Intermediation	
Label	Enter a name to uniquely identify the basic authentication intermediation. No external mapping is made to the label value.
Credential Type	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • System—Specifies the set of user credentials, such as primary and secondary authorization credentials, stored in the device. If you select this option, you do not need to enter the username and password. • Variable—Allows tokens such as username and password to be used in the Username and Password boxes. • Static—Specifies the username and password exactly as they are entered in the Username and Password boxes.

Table 59: Configuring Basic, NTLM, and Kerberos Resources (*continued*)

Options	Your Action
Username	Enter the account username. If you select Variable as the credential type, you can enter the username token.
Password	Enter an account password.
Variable Password	Enter the password token if you select Variable as the credential type.
Pattern	Enter the hostnames mapped to the Kerberos realm. You can enter wildcard characters, such as *.y.com, *.kerber.net, or *.*

**Related
Documentation**

- [Defining a Basic Authentication, NTLM, or Kerberos Intermediation Resource Policy \(NSM Procedure\) on page 221](#)
- [Configuring a SAML Access Control Resource Policy \(NSM Procedure\) on page 223](#)
- [Configuring SAML SSO Artifact Profile Resource Policy \(NSM Procedure\) on page 226](#)

Defining a Basic Authentication, NTLM, or Kerberos Intermediation Resource Policy (NSM Procedure)

Basic authentication, NT LAN Manager (NTLM), or Kerberos intermediation resource policies enable you to control NTLM and Kerberos intermediation on the Secure Access device. If a user accesses a Web resource that sends a basic authentication challenge, the device intercepts the challenge, displays an intermediate sign-in page to collect the credentials for the Web resource, and then rewrites the credentials along with the entire challenge or response sequence.

With the Kerberos intermediation resource policy, backend Web applications protected by Kerberos are accessible to end users. For example, a user logs in to the device using Active Directory as the authentication server and the authentication protocol is Kerberos. When the user browses a Kerberos-protected server, the user is single signed on to the backend server and is not prompted for any credentials. A user logs in to the device using an authentication protocol other than Kerberos and then browses a Kerberos-protected server. Depending on the Kerberos intermediation resource policy settings and the configured Kerberos authentication server, the user is either authenticated by the system or is prompted to enter a username and password.

To define a basic authentication, NTLM, or Kerberos intermediation resource policy:

1. In the navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure a basic, NTLM, or Kerberos intermediation resource policy.
3. Click the **Configuration** tab. Select **Users > Resource Policies > Basic Auth/NTLM SSO**.
4. Click the **New** icon to configure the options as described in [Table 60 on page 222](#).
5. Click **OK** to save the changes.

Table 60: Basic Authentication, NTLM, or Kerberos Intermediation Policy

Options	Your Action
General tab	
Name	Enter a name to label the policy.
Description	Enter a description for the policy.
Resources	Enter the resource name to which this policy applies.
Applies to roles	<p>Select any of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • All—Allows you to apply this policy to all users. • Selected—Allows you to apply this policy only to users who are mapped to roles in the Members list. In the Roles tab, you must add roles as members, from the Non-members list. • Except those selected—Allows you to apply this policy to all users except for the users who map to the roles in the Members list.
Authentication Type	<p>Select any of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • Disable SSO—Specifies that the device disables the automatic SSO authentication for this user role, and prompts the user for sign-in credentials. • Basic Authentication—Specifies that the device uses the basic authentication intermediation method to control the SSO behavior. • Disable Intermediation (Not valid for web proxies)—Specifies that in selecting this option, the device does not intermediate the challenge or response sequence. • NTLM Authentication—Specifies that the device uses the Microsoft NTLM intermediation method to control the SSO behavior. • Kerberos Authentication—Specifies that the device uses the Kerberos intermediation method to control the SSO behavior. • Constrained Delegation—Specifies that the device uses the constrained delegation intermediation method to control the SSO behavior. • Detailed Rules—Allows you to specify one or more detailed rules for this policy.
Label	Enter a label name for the basic, NTLM, or Kerberos authentication types, and the constrained delegation.
Fallback to NTLM V1	Select the Fallback to NTLM V1 check box to enable this option.
Fallback to NTLM V2	Select the Fallback to NTLM V2 check box to enable this option.
Fallback to Kerberos	Select the Fallback to Kerberos check box to enable this option.
Roles tab	
Roles	<p>Select roles to access resource policies.</p> <p>NOTE: This tab is enabled only when you select Selected or Except those selected from the Applies to roles drop-down list.</p>
Detailed Rules tab	

Table 60: Basic Authentication, NTLM, or Kerberos Intermediation Policy (*continued*)

Options	Your Action
Detailed Rule	Enter the detailed rule information as described in the General tab section of Table 60 on page 222 .
Conditions	Click New Expression and enter a condition name for the rule. You can also set conditions for the rule. Conditions include logical operators, prebuilt expressions, variables, and so on.

Related Documentation

- [Configuring a SAML Access Control Resource Policy \(NSM Procedure\) on page 223](#)
- [Configuring SAML SSO Artifact Profile Resource Policy \(NSM Procedure\) on page 226](#)
- [Configuring Basic, NTLM, and Kerberos Resources \(NSM Procedure\) on page 218](#)

Configuring a SAML Access Control Resource Policy (NSM Procedure)

When enabling access control transactions to a trusted access management system, the Secure Access device and trusted access management system exchanges information.

To configure a SAML access control resource policy:

1. In the navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure a SAML access control resource policy.
2. Click the **Configuration** tab. Select **Users > Resource Policies > Web > SAML ACL**.
3. Add or modify settings as specified in [Table 61 on page 223](#).
4. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 61: Configuring SAML Access Control Resource Policy Details

SAML ACL > General tab or Detailed Rule tab		
Name	Specifies the name of the policy.	Enter the name.
Description	Describes the policy.	Enter the policy.
New Resources	Specifies the resources to which this policy applies.	Enter the resources.

Table 61: Configuring SAML Access Control Resource Policy Details (*continued*)

Role application	Specifies the roles to which this policy applies.	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • Policy applies to ALL roles—Applies this policy to all users. • Policy applies to SELECTED roles—Applies this policy only to users who are mapped to roles in the selected roles list. • Policy applies to all roles OTHER THAN those selected below—Applies this policy to all users except for those who map to the roles in the selected roles list.
Action	Allows or denies the Secure Access device to perform an access control check.	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • Use SAML—Secure Access device performs an access control check to the specified URL. • Do not use SAML—Secure Access device does not perform an access control check. • Use Detailed Rules—Specifies one or more detailed rules for this policy.
SAML Web Service URL	Specifies the URL of the access management system's SAML server.	Enter the URL, using the format:https://hostname/ws.
SAML Web Service Issuer	Specifies the hostname of the issuer, which in most cases is the hostname of the access management system.	Enter a unique string.
Authentication Type	Specifies the authentication method that the SAML Web service should use to authenticate the Secure Access device.	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • None—Does not authenticate the Secure Access device. • Username/Password—Authenticates the Secure Access device using a username and password. • Certificate—Authenticates the Secure Access device using a certificate signed by a trusted certificate authority.

Table 61: Configuring SAML Access Control Resource Policy Details (*continued*)

Username	Specifies the username that the Secure Access device must send the Web service. NOTE: The username and password fields are displayed only when you select the Username/Password option from the Authentication Type drop-down list.	Enter the username.
Password	Specifies the password that the Secure Access device must send the Web service.	Enter the password
Certificate	Specifies the certificate installed on the Secure Access device to send to the Web service. NOTE: This box is displayed only when you select Certificate option from the Authentication Type drop-down list.	Select the certificate installed on the Secure Access device from the drop-down list.
Subject Name Type	Specifies which method the Secure Access device and SAML Web service should use to identify the user.	Select one of the following options from the drop-down list: <ul style="list-style-type: none"> • Other—Sends the username in another format agreed upon by the Secure Access device and the SAML Web service. • DN—Sends the username in the format of a DN (distinguished name) attribute. • Email Address—Sends the username in the format of an e-mail address. • Windows—Sends the username in the format of a Windows domain qualified username.
Subject Name	Specifies the username that the Secure Access device should pass to the SAML Web service.	Enter the username.
Device Issuer	Specifies the hostname of the issuer, which in most cases is the hostname of the access management system.	Enter the hostname.
Maximum Cache Time (seconds)	Specifies the amount of time the Secure Access device should cache the responses (in seconds).	Enter the time.

Table 61: Configuring SAML Access Control Resource Policy Details (*continued*)

Ignore Query data	Specifies that the Secure Access device should remove the query string from the URL before requesting authorization or caching the authorization response.	Select the Ignore Query data check box to enable this feature.
SAML ACL > Role		
Role	Maps roles to access control policy resources. NOTE: The Role tab is enabled only when you select Policy applies to SELECTED roles or Policy applies to all roles OTHER THAN those selected below from the Action drop-down list.	Select a role and click Add to add roles from the Non-members to the Members list.
SAML ACL > Detailed Rules tab		
Conditions	Specifies one or more expressions to evaluate to perform the action.	Specify one of the following options: <ul style="list-style-type: none"> Boolean expressions: Using system variables, write one or more Boolean expressions using the NOT, OR, or AND operators. Custom expressions: Using the custom expression syntax, write one or more custom expressions.

- Related Documentation**
- [Configuring SAML SSO Artifact Profile Resource Policy \(NSM Procedure\) on page 226](#)
 - [Setting Up Secure Access Device Host Checker Options \(NSM Procedure\) on page 231](#)

Configuring SAML SSO Artifact Profile Resource Policy (NSM Procedure)

Configure SAML SSO Artifact profile resource policy to communicate using the artifact profile (also called Browser/Artifact profile) the trusted access management server “pulls” authentication information from the Secure Access device.

To configure SAML SSO artifact profile resource policy:

1. In the navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure a SAML Artifact Profile resource policy.
2. Click the **Configuration** tab. Select **Users > Resource Policies > Web > SAML SSO**.
3. Add or modify settings as specified in [Table 62 on page 227](#).
4. Click one:
 - **OK**—Saves the changes.

- **Cancel**—Cancels the modifications.

Table 62: Configuring SAML SSO Artifact Profile Resource Policy Details

Option	Function	Your Action
SAML SSO > General tab or Detailed Role tab		
Name	Specifies the name of the policy.	Enter the name.
Description	Describes the policy.	Enter the description.
New Resources	Specifies the resources to which this policy applies.	Enter the path
Role application	Specifies the roles to which this policy applies.	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • Policy applies to ALL roles—Applies the policy to all users. • Policy applies to SELECTED roles—Applies the policy only to users who are mapped to roles in the Role Selection section. • Policy applies to all roles OTHER THAN those selected below—Applies the policy to all users except for those who mapped to the roles in the Role Selection section.
Action	Specifies that the Secure Access device performs a single-sign on (SSO) request to the specified URL.	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • Use SAML SSO—Secure Access device performs a single-sign on (SSO) request to the specified URL using the data specified in the SAML SSO details section. • Do not use SAML SSO—Secure Access device does not perform an SSO request. • Use Detailed Rules—Specifies one or more detailed rules for this policy.

Table 62: Configuring SAML SSO Artifact Profile Resource Policy Details (*continued*)

Option	Function	Your Action
SAML Assertion Consumer service URL	Specifies the URL that the Secure Access device must contact the assertion consumer service during SSO transactions.	Enter the URL.
Profile	Specifies the type of the profile.	Select Artifact or POST from the drop-down list.
Source ID	Specifies the source ID for the Secure Access device.	Enter the source ID. If you enter a: <ul style="list-style-type: none"> • Plain text string—The Secure Access device converts, pads, or truncates it to a 20-byte string. • Base-64 encoded string—The Secure Access device decodes it and ensures that it is 20 bytes.
Issuer	Specifies the string that the Secure Access device can use to identify itself when it generates assertions.	Enter the string.
Subject Name Type	Specifies which method the Secure Access device and assertion consumer service should use to identify the user.	Select one of the following options from the drop-down list: <ul style="list-style-type: none"> • Other—Sends the username in another format • DN—Sends the username in the format of a DN (distinguished name) attribute. • Email Address—Sends the username in the format of an e-mail address. • Windows—Sends the username in the format of a Windows domain qualified username.
Subject Name	Specifies the username that the Secure Access device should pass to the assertion consumer service.	Enter a variable. Or, enter static text.
New Cookie Domain(s)	Specifies the list of domains to which the SSO cookies are associated.	Enter a comma-separated list of domains.

Table 62: Configuring SAML SSO Artifact Profile Resource Policy Details (*continued*)

Option	Function	Your Action
Authentication Type	Specifies the authentication method that the Secure Access device should use to authenticate the assertion consumer service.	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • None—Does not authenticate the assertion consumer service. • Username/Password—Authenticates the assertion consumer service using a username and password. • Certificate—Authenticates the assertion consumer service using certificate attributes.
Username	<p>Specifies the username that the assertion consumer service must send the Secure Access device.</p> <p>NOTE: The username and password boxes are displayed only when you select the Username/Password option from the Authentication Type drop-down list.</p>	Enter the username.
Password	Specifies the password that the Secure Access device must send the Secure Access device.	Enter the password.
Certificate		
Attribute Name	<p>Specifies the attributes that the assertion consumer service must send the Secure Access device. (one attribute per line).</p> <p>NOTE: The certificates-attributes box is displayed only when you select Certificate option from the Authentication Type drop-down list.</p>	Enter the attribute name. For example, enter cn=sales.
Attribute Value	Specifies the attribute values that match the values contained in the assertion consumer service's certificate.	Enter the attribute value.
SAML SSO > Role		

Table 62: Configuring SAML SSO Artifact Profile Resource Policy Details (*continued*)

Option	Function	Your Action
Role	<p>Maps roles to the resource control policy.</p> <p>NOTE: The Role tab is enabled only when you select the Policy applies to SELECTED roles or the Policy applies to all roles OTHER THAN those selected below option from the Applies to role drop-down list.</p>	<p>Select a role and click Add to add roles from the Non-members to Members list.</p>
SAML SSO > Detailed Role		
Conditions	<p>Specifies one or more expressions to evaluate to perform the action.</p>	<p>Specify one of the following options:</p> <ul style="list-style-type: none"> • Boolean expressions: Using system variables, write one or more Boolean expressions using the NOT, OR, or AND operators. • Custom expressions: Using the custom expression syntax, write one or more custom expressions.

Related Documentation

- [Setting Up Secure Access Device Host Checker Options \(NSM Procedure\) on page 231](#)
- [Configuring a SAML Access Control Resource Policy \(NSM Procedure\) on page 223](#)

Configuring Secure Access Host Checker Policies

- [Setting Up Secure Access Device Host Checker Options \(NSM Procedure\) on page 231](#)
- [Configuring General Host Checker Remediation \(NSM Procedure\) on page 233](#)
- [Configuring Host Checker Third-Party Applications Using Predefined Rules \(NSM Procedure\) on page 234](#)
- [Configuring the Remote Integrity Measurement Verifier Server \(NSM Procedure\) on page 240](#)
- [Configuring Host Checker Customized Requirements Using Custom Rules \(NSM Procedure\) on page 241](#)
- [Enabling Advanced Endpoint Defense \(NSM Procedure\) on page 246](#)
- [Enabling Predefined Client-Side Policies for Windows Only \(NSM Procedure\) on page 247](#)
- [Configuring Virus Signature Version Monitoring \(NSM Procedure\) on page 248](#)
- [Importing Virus Signature Version Monitoring or Patch Management Version Monitoring List \(NSM Procedure\) on page 249](#)
- [Assigning a Proxy Server an Auto-Update Server \(NSM Procedure\) on page 249](#)

Setting Up Secure Access Device Host Checker Options (NSM Procedure)

You can specify global options for Host Checker that apply to any user for whom Host Checker is required in an authentication policy or a role mapping rule.

To specify general Host Checker options:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to specify general Host Checker options.
3. Click the **Configuration** tab. In the configuration tree, select **Authentication > Endpoint Security > Host Checker > Settings** tab.
4. Add or modify Host Checker settings as specified in [Table 63 on page 232](#).
5. Click one:
 - **OK**—Saves the changes.

- **Cancel**—Cancels the modifications.

Table 63: Host Checker Options Configuration Details

Option	Function	Your Action
Perform check every (minutes)	Specifies the interval at which you want the Host Checker to perform policy evaluation on a client machine.	Enter the interval in minutes. NOTE: If you enter a value of zero, Host Checker runs only on the client machine when the user first signs into the Secure Access device.
Client-side process, login inactivity timeout (minutes)	Specifies an interval to control timing out in the following situations: <ul style="list-style-type: none"> • If the user navigates away from the Secure Access device sign-in page after Host Checker starts running but before signing in to the Secure Access device, Host Checker continues to run on the user's machine for the interval you specify. • If the user is downloading Host Checker over a slow connection, increase the interval to allow enough time for the download to complete. 	Enter the interval in minutes.
Auto-upgrade Host Checker	Secure Access device automatically downloads the Host Checker application to a client computer when the version of Host Checker on the Secure Access device is newer than the version installed on the client.	Select the Auto-upgrade Host Checker to enable this feature.
Perform dynamic policy reevaluation	Secure Access device automatically refreshes the roles of individual users by enabling dynamic policy evaluation for Host Checker.	Select the Perform dynamic policy reevaluation to enable this feature.

Related Documentation

- [Configuring General Host Checker Remediation \(NSM Procedure\) on page 233](#)
- [Configuring Host Checker Third-Party Applications Using Predefined Rules \(NSM Procedure\) on page 234](#)

Configuring General Host Checker Remediation (NSM Procedure)

You can specify general remediation actions that you want the Host Checker to take if an endpoint does not meet the requirements of a policy. For example, you can display a remediation page to the user that contains specific instructions and links to resources to help the user bring their endpoint into compliance with Host Checker policy requirements.

To configure general Host Checker remediation:

1. In the navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure general Host Checker remediation.
2. Click the **Configuration** tab. Select **system > Authentication > Endpoint Security**.
3. In the Endpoint Security screen, select **Settings > Policies** and click the **Add** icon.
4. Create new client-side policies and enable customized server-side policies.
5. Click the tab that corresponds to the operating system for which you want to specify Host Checker options—**Windows, Mac, Linux, Solaris, or Windows Mobile**.
6. Add or modify settings as specified in [Table 64 on page 233](#) to specify the remediation actions that you want Host Checker to perform if a user's computer does not meet the requirements of the current policy.
7. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 64: Configuring General Host Checker Remediation Details

Option	Function	Your Action
Remediation tab		
Enable Custom Instructions	Specifies the instructions you want to display to the user on the Host Checker remediation page.	<p>Select the Enable Custom Instructions option to enable this feature, and then enter the instructions.</p> <p>NOTE: You can use the following HTML tags to format text and add links to resources such as policy servers or web sites: <code><i></code>, <code></code>, <code>
</code>, <code></code>, and <code><a href></code>.</p>
Enable Custom Actions	Allows you to select one or more alternate policies that you want Host Checker to evaluate if the user's computer does not meet the current policy requirements. The alternate policy must be either a third-party policy that uses a J.E.D.I. package or a Secure Virtual Workspace policy.	Select the Enable Custom Actions option to enable this feature, and then select the alternate policy and click Add to move from the Non-members to the Members list.

Table 64: Configuring General Host Checker Remediation Details (continued)

Option	Function	Your Action
Kill Processes	Specifies the name of one or more processes you want to kill if the user's computer does not meet the policy requirements. You can include an optional MD5 checksum for the process.	Select the Kill Processes option to enable this feature, and then enter the name. For example, enter <code>keylogger.exe</code>
Delete Files	Specifies the names of files you want to delete if the user's computer does not meet the policy requirements. Enter one filename per line.	Select the Delete Files option to enable this feature, and then enter the filename. For example, enter <code>c:\temp\bad-file.txt</code> <code>/temp/bad-file.txt</code> .
Send reason strings	Displays a message to users (called a reason string) that is returned by Host Checker or integrity measurement verifier (IMV) and explains why the client machine does not meet the Host Checker policy requirements. NOTE: This option applies to predefined rules, custom rules, and to third-party IMVs that use extensions in the Juniper Networks TNC SDK.	Select the Send reason strings option to enable this feature.

Related Documentation

- [Configuring Host Checker Third-Party Applications Using Predefined Rules \(NSM Procedure\) on page 234](#)
- [Configuring the Remote Integrity Measurement Verifier Server \(NSM Procedure\) on page 240](#)
- [Setting Up Secure Access Device Host Checker Options \(NSM Procedure\) on page 231](#)

Configuring Host Checker Third-Party Applications Using Predefined Rules (NSM Procedure)

Host Checker comes pre-equipped with a vast array of predefined rules that check for antivirus software, firewalls, malware, spyware, and specific operating systems from a wide variety of industry leaders. You can enable one or more of these rules within a Host Checker client-side policy to ensure that the integrated third-party applications that you specify are running on your users' computers in accordance with your specifications. For firewall and antivirus rules, you can specify remediation actions to automatically bring the endpoint into compliance.

To configure third-party applications using predefined rules:

1. In the navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure Host Checker third-party applications using predefined rules.

3. Click the **Configuration** tab and select **Authentication > Endpoint Security > Host Checker**. The corresponding workspace appears.
4. Create a new policy or click an existing policy in the Policies section of the page.
5. Click the tab that corresponds to the operating system for which you want to specify Host Checker options—**Windows, Mac, Linux, Solaris and Windows Mobile**. In the same policy, you can specify different Host Checker requirements for each operating system.
6. Add and modify settings as specified in [Table 65 on page 235](#).
7. Specify the support products or vendors for a system scan check.
8. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 65: Configuring Host Checker Third-Party Applications Using Predefined Rules Details

Option	Function	Your Action
Predefined Antivirus Rules		
Rule Name	Specifies the name for Antivirus rule.	Enter the rule name.
Select Products	Specifies the support products or vendors for system scan check.	Select one of the following options: <ul style="list-style-type: none"> • Require any supported product—Specifies the software vendor's product that is supported for the system scan check. • Require specific products/Vendors—Specifies the specific vendor for the system scan check.
Require any supported product from a specific vendor	Checks for any product (rather than requiring you to select every product separately).	Select the Require any supported product from a specific vendor to enable this feature.
Require specific products	Checks for specific products/vendors to define compliance by allowing any product by a specific vendor (for example, any Symantec product).	Select the Require specific products to enable this feature.
Enable Scan period check	Enables the System scan for the product.	Select the Enable Scan period check to enable this feature.
Successful System Scan must have been performed in the last: (days)	Specifies the days to perform the system scan.	Enter the days.

Table 65: Configuring Host Checker Third-Party Applications Using Predefined Rules Details (*continued*)

Option	Function	Your Action
Consider this rule as passed if 'Full System Scan' was started successfully as remediation.	Passes the rule if system full scan starts successfully as remediation.	Select the Consider this rule as passed if 'Full System Scan' was started successfully as remediation. to enable this feature.
Enable virus definitions update check	Checks for the viral updates.	Select the Enable virus definitions update check to enable this feature.
Virus Definition files should not be older than (updates)	Specifies the update of client Virus definition files the client must use.	Enter a number between 1 and 10. For example: If you enter 1, the client must have the latest update. You must import the virus signature list for the supported vendor.
Monitor this rule for change in result	Continuously monitors the policy compliance of endpoints.	Select the Monitor this rule for change in result to enable this feature.
Enable Download latest virus definition files for all supported products	Allows you to download latest virus definition files for all supported products.	Select the Enable Download latest virus definition files for all supported products to enable this feature.
Enable Turning on Real Time Protection for all supported products	Enables turning on real time protection for all supported products.	Select the Enable Turning on Real Time Protection for all supported products to enable this feature.
Enable Starting of Antivirus Scan for all supported products	Scans supported products with antivirus scan.	Select the Enable Starting of Antivirus Scan for all supported products to enable this feature.
Selected Vendors tab		
Selected Vendors	Allows you to select the specific vendors.	Select the vendor, and then click Add to move the vendor from the Non-members to the Members list.
Specific Products Selected tab		
Specific Products Selected	Allows you to select the specific products.	Select the product, and then click Add to move the product from the Non-members to the Members list.
Selected Products tab		
Product name	Allows you to select the product.	Select the product from the Product name drop-down list.
live-update	Allows live-update for the product.	Select the live-update option to enable this feature.

Table 65: Configuring Host Checker Third-Party Applications Using Predefined Rules Details (*continued*)

Option	Function	Your Action
set-real-time-protection-on	Allows real-time protection for the product.	Select the set-real-time-protection on option to enable this feature.
start-scan	Starts the scanning process for the product.	Select the start-scan option to enable this feature.
Predefined Firewall Rules		
Rule Name	Specifies the name for the firewall rule.	Enter the name.
Select Products	Allows you to select your firewall vendor(s) and product(s).	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • Require any supported product—Specifies the software vendor's product that is supported for the system scan check. • Require specific products/vendors—Specifies the specific vendor for the system scan check.
Require any supported product from a specific vendor	Checks for any product (rather than requiring you to select every product separately)	Select the Require any supported product from a specific vendor to enable this feature.
Require specific products	Specifies specific products/vendors, and defines compliance by allowing any product by a specific vendor (for example, any Symantec product).	Select the Require specific products to enable this feature.
Monitor this rule for change in result	Continuously monitors the policy compliance of endpoints.	Select the Monitor this rule for change in result to enable this feature.
Turn on firewall for all supported products	Turns on the Firewall.	Select the Turn on firewall for all supported products to enable this feature.
Selected Vendors tab		
Selected Vendors	Allows you to select the specific vendors.	Select the vendor, and then click Add to move the vendor from the Non-members to the Members list.
Specific Products Selected tab		

Table 65: Configuring Host Checker Third-Party Applications Using Predefined Rules Details (*continued*)

Option	Function	Your Action
Specific Products Selected	Allows you to select the specific products.	Select the product, and then click Add to move the product from the Non-members to the Members list.
Selected Products		
Product name	Allows you to select the product.	Select the product from the Product name drop-down list.
turn-on-firewall	Turns on the Firewall for the product.	Select the turn-on-firewall option to enable this feature.
Predefined Malware Rules		
Rule Name	Specifies the name of the Malware rule.	Enter the Malware rule name.
Monitor this role for change in result	Continuously monitors the policy compliance of endpoints.	Select the Monitor this role for change in result to enable this feature.
Selected Products	Allows you to select the products.	Select the product, and then click Add to enable this feature.
Predefined Spyware Rules		
Rule Name	Enter the name for the spyware rule.	Enter the name.
Select Products	Allows you to select products or vendors	Select one of the following options from the drop-down list: <ul style="list-style-type: none"> • Require any supported product—Specifies the software vendor's product that is supported for the system scan check. • Require specific products/vendors—Specifies the specific vendor for the system scan check.
Require any supported product from a specified vendor	Checks for any product (rather than requiring you to select every product separately).	Select the Require any supported product from a specific vendor option to enable this feature.

Table 65: Configuring Host Checker Third-Party Applications Using Predefined Rules Details (*continued*)

Option	Function	Your Action
Require specific products	Specifies specific products/vendors, and defines compliance by allowing any product by a specific vendor (for example, any Symantec product).	Select the Require specific products option to enable this feature.
Monitor this rule for change in result	Continuously monitors the policy compliance of endpoints.	Select the Monitor this rule for change in result option to enable this feature.
Selected Vendors tab		
Selected Vendors	Allows you to select the vendors.	Select the vendor, and then click Add to move the vendor from the Non-members to the Members list.
Specific Products Selected tab		
Specific Products Selected	Allows you to select specific products.	Select the product, and then click Add to move the product from the Non-members to the Members list.
Selected Products		
Product name	Allows you to select the product.	Select the product from the Product name drop-down list.
Predefined OS Checks Rules		
Rule Name	Specifies the name for the OS Checks rule.	Enter the name.
OS Selections	Specifies the operating systems.	Select the operating system, and then click Add to move from the Non-members to the members list.

Related Documentation

- [Configuring the Remote Integrity Measurement Verifier Server \(NSM Procedure\) on page 240](#)
- [Configuring Host Checker Customized Requirements Using Custom Rules \(NSM Procedure\) on page 241](#)
- [Configuring General Host Checker Remediation \(NSM Procedure\) on page 233](#)

Configuring the Remote Integrity Measurement Verifier Server (NSM Procedure)

The Trusted Network Connect (TNC) standard enables the enforcement of security requirements for endpoints connecting to networks. The client-side components of the TNC are the IMCs and the TNC-client (TNCC). The TNCC compiles the IMC measurements and sends them to the server. At the server, there is a corresponding set of components: the TNC-server (TNCS) and the IMVs. The TNCS manages the messages between the IMVs and the IMCs and sends the recommendations, based on the IMVs, to the policy engine.

To configure the remote IMV server so that the Secure Access device can communicate with it:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure the remote IMV server.
3. Click the **Configuration** tab. In the configuration tree, select **Authentication > Endpoint Security > Host Checker**.
4. Add or modify settings as specified in [Table 66 on page 240](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 66: Configuring the Remote IMV Server Details

Option	Function	Your Action
Remote IMV > Remote IMV Servers		
Name	Specifies the name for the server.	Enter the name for the remote IMV server.
Description	Describes about the server.	Enter a brief description about the server.
Host	Specifies the hostname.	Enter either the IP address or hostname as defined in the server certificate.
Port	Specifies the port number that the Secure Access device uses to communicate with the remote IMV server.	Enter a unique port number. NOTE: Ensure that no other service is using this port number. The default port number is the same as the default https port number.
Shared secret	Specifies the shared secret information.	Enter the same shared secret used in the client information entry on the remote IMV server.

Table 66: Configuring the Remote IMV Server Details (*continued*)

Option	Function	Your Action
Remote IMV > Remote IMVs		
Name	Specifies the name of the IMV.	Enter the name for the remote IMVs.
Description	Describes the IMV.	Enter a brief description about the IMV.
IMV Name	Specifies the IMV name that matches the “human readable name” in the IMV’s well-known registry key on the remote IMV server.	Enter a name for the IMV.
Primary Server	Specifies the primary remote IMV server where the IMV is installed.	Select the primary remote IMV server from the drop-down list.
Secondary Server	Specifies the secondary remote IMV server where the IMV is installed. NOTE: The secondary server acts as a failover in case the primary server becomes unavailable.	Select the secondary remote IMV server from the drop-down list.

- Related Documentation**
- [Configuring Host Checker Customized Requirements Using Custom Rules \(NSM Procedure\) on page 241](#)
 - [Configuring a Secure Application Manager Resource Policy \(NSM Procedure\) on page 143](#)

Configuring Host Checker Customized Requirements Using Custom Rules (NSM Procedure)

You can create custom rules within a Host Checker policy to define requirements that users' computers must meet. And creating these custom rules happens only if the predefined client-side policies and rules do not meet the needs.

To configure customized requirements using custom rules:

1. In the navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure customized requirements using custom rules.
3. Click the **Configuration** tab and select **Authentication > Endpoint Security > Host Checker**. The corresponding workspace appears.
4. Create a new policy or click an existing policy in the Policies section of the page.
5. Click the tab that corresponds to the operating system for which you want to specify Host Checker options—**Windows**, **Mac**, **Linux**, **Solaris**, or **Windows Mobile**. In the same policy, you can specify different Host Checker requirements for each operating system.

6. Configure the customized requirements using custom rules using the settings described in [Table 67 on page 242](#).
7. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 67: Configuring Host Checker Customized Requirements Using Custom Rules Details

Option	Function	Your Action
Settings tab		
Remote IMV Rules	IMV—Use this rule type to configure integrity measurement software that a client must run to verify a particular aspect of the client's integrity, such as the client's operating system, patch level, or virus protection.	<ol style="list-style-type: none"> 1. Enter the rule name. 2. Select the IMV. 3. Click OK.
NHC Rules	(Windows only)—Use this rule type to specify the location of a custom DLL. Host Checker calls the DLL to perform customized client-side checks. If the DLL returns a success value to Host Checker, then the Secure Access device considers the rule met.	<ol style="list-style-type: none"> 1. Enter the rule name, vendor name, and the path to NHC DLL on client machines. 2. Select the Monitor this rule for change in result check box to continuously monitor the policy compliance of endpoints. 3. Click OK.
Ports Rules	Use this rule type to control the network connections that a client can generate during a session. This rule type ensures that certain ports are open or closed on the client machine before the user can access the Secure Access device.	<ol style="list-style-type: none"> 1. Enter the rule name. 2. Select the Required option to specify that these ports are open or closed. 3. Enter a comma delimited port list (without spaces) of ports or port ranges, such as: 1234,11000-11999,1235. 4. Click Ok.
Process Rules	Use this rule type to control the software that a client may run during a session. This rule type ensures that certain processes are running or not running on the client machine before the user can access resources protected by the Secure Access device.	<ol style="list-style-type: none"> 1. Enter the rule name. 2. Select the Required option to specify that these ports are open or closed. 3. Enter the process name (executable file), such as: good-app.exe. 4. Enter the MD5 checksums value of each executable file to which you want the policy to apply (optional). 5. Select the Monitor this rule for change in result check box to continuously monitor the policy compliance of endpoints. 6. Click OK.

Table 67: Configuring Host Checker Customized Requirements Using Custom Rules Details (*continued*)

Option	Function	Your Action
Settings tab		
File Rules	Use this rule type to ensure that certain files are present or not present on the client machine before the user can access the Secure Access device . You may also use file checks to evaluate the age and content (through MD5 checksums) of required files and allow or deny access accordingly.	<ol style="list-style-type: none"> 1. Enter the rule name. 2. Enter the filename such as: c:\temp\bad-file.txt or /temp/bad-file.txt. 3. Select the Required option to specify that these ports are open or closed. 4. Enter the minimum version of the file (optional). For example, if you require notepad.exe to be present on the client, you can enter 5.0 in the box. Host Checker accepts version 5.0 and later, of notepad.exe. 5. Enter the maximum age of files in the File modified less than (days ago) box. 6. Enter the MD5 checksums value of each executable file to which you want the policy to apply (optional). 7. Select the Monitor this rule for change in result check box to continuously monitor the policy compliance of endpoints. 8. Click OK.
Registry Rules	(Windows only)—Use this rule type to control the corporate PC images, system configurations, and software settings that a client must have to access the Secure Access device. This rule type ensures that certain registry keys are set on the client machine before the user can access the Secure Access device. You may also use registry checks to evaluate the age of required files and allow or deny access accordingly.	<ol style="list-style-type: none"> 1. Enter the rule name. 2. Select the registry root key from the drop-down list. 3. Enter the path to the application folder for the registry subkey. 4. Enter the name of the key's value. 5. Select the key value's type (String, Binary, or DWORD) from the drop-down list (optional). 6. Enter the registry value. 7. Select the Set Registry value specified in the criteria check box. 8. Select the Monitor this rule for change in result check box to continuously monitor the policy compliance of endpoints. 9. Click OK.

Table 67: Configuring Host Checker Customized Requirements Using Custom Rules Details (*continued*)

Option	Function	Your Action
Settings tab		
NetBIOS Rules	(Windows only, does not include Windows Mobile)—Use this rule type to check the NetBIOS name of the client machine before the user can access the Secure Access device.	<ol style="list-style-type: none"> 1. Enter the rule name. 2. Select the Required option to require that NETBIOS name of the client machine matches or does not match any one of the names you specify. 3. Enter a comma-delimited list (without spaces) of NetBIOS names. The name can be up to 15 characters in length. You can use wildcard characters in the name and it is not case-sensitive. For example: md*, m*xp and *xp all match MDXP. 4. Click OK.
MAC Address Rules	(Windows only)—Use this rule type to check the MAC addresses of the client machine before the user can access the Secure Access device.	<ol style="list-style-type: none"> 1. Enter the Rule Name. 2. Select the Required option to require that a MAC address of the client machine matches or does not match any of the addresses you specify. 3. Enter a comma-delimited list (without spaces) of MAC addresses in the form XX:XX:XX:XX:XX:XX where the X's are hexadecimal numbers. For example: 00:0e:1b:04:40:29. 4. Click OK.
Machine Certificate Rules	(Windows only)—Use this rule type to check that the client machine is permitted access by validating the machine certificate stored on the client machine.	<ol style="list-style-type: none"> 1. Enter the rule name. 2. From the Select Issuer Certificate list, select the certificate that you want to retrieve from the user's machine and validate. Or, select Any Certificate to skip the issuer check and only validate the machine certificate based on the optional criteria that you specify below. 3. Enter any additional criteria that Host Checker should use when verifying the machine certificate in the Certificate field and Expected value box. 4. Click OK.
Patch Assessment Rules		

Table 67: Configuring Host Checker Customized Requirements Using Custom Rules Details (*continued*)

Option	Function	Your Action
Settings tab		
Scan for Specific products	Configures a policy based on specific products.	<ul style="list-style-type: none"> Select one of the following options from the drop-down list <ul style="list-style-type: none"> Enter the integrity measurement rule name. All products—Host Checker checks for all of the exposed patches on the endpoint. Specific products—An extensive listing of products and versions. Select specific patches that you wish to ignore for all products by clicking the Add button under Ignore following patches. Select the check boxes to determine the severity level of the patches that you wish to ignore. Select the Enable SMS patch update check box to update patches using SMS.
Scan for specific patches	Configures a policy based on specific patches	<ul style="list-style-type: none"> Enter the integrity measurement rule name. Select the specific patches and then click Add to move the patches from the Non-members to the Members list. Select the Enable SMS patch update check box to update patches using SMS.

- Related Documentation**
- [Configuring Global Cache Cleaner Options \(NSM Procedure\) on page 251](#)
 - [Configuring a Secure Application Manager Resource Policy \(NSM Procedure\) on page 143](#)

Enabling Advanced Endpoint Defense (NSM Procedure)

Host Checker includes integrated antispyware functionality that can detect and remediate Windows endpoints with spyware and keyloggers. Advanced endpoint defense (AED) ensures that malware, spyware, viruses, or worms are not present on endpoints that attempt to connect to the device, and you can restrict or quarantine these endpoints depending on your Host Checker policy configuration.

AED can scan endpoints and provide real-time file system write and execution to automatically remediate machines. AED reports any threats that are detected along with the remediation status.

To enable and use AED antispyware:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to enable the AED antispyware.
2. Click the **Configuration** tab. In the **Configuration** tree, select **Authentication > Endpoint Security > Host Checker**.
3. Select **Settings > Policies**, and then click **New**.
4. Enter a name for the policy in the Policy Name box.
5. In the Policy Type list, select **Advanced Endpoint Defense Policy**.
6. In the Policy Info page, select the **Enable Signature definitions** check box. This sets the age of the signature definitions database.
7. Enter the frequency in the Check that Signature definitions are updated in (days) box. This function does not change the frequency of updates. This number determines the maximum permissible age of signatures.
8. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.



NOTE: When you create or configure realm or role Host Checker restrictions, you can select **Advanced Endpoint Defense: Malware Protection** to apply to that role or realm.

Related Documentation

- [Configuring Host Checker Customized Requirements Using Custom Rules \(NSM Procedure\) on page 241](#)
- [Enabling Predefined Client-Side Policies for Windows Only \(NSM Procedure\) on page 247](#)

Enabling Predefined Client-Side Policies for Windows Only (NSM Procedure)

The Secure Access device comes equipped with predefined client-side Host Checker policies that you simply need to enable, not create or configure, to use them. The connection control policies work only on Windows systems. It includes:

- [Enabling Connection Control Policies on page 247](#)

Enabling Connection Control Policies

The predefined connection control Host Checker policy prevents attacks on Windows client computers from other infected computers on the same physical network. The Host Checker connection control policy blocks all incoming TCP connections. This policy allows all outgoing TCP and Network Connect traffic, as well as all connections to DNS servers, WINS servers, DHCP servers, proxy servers, and the Secure Access device.



NOTE: Users must have administrator privileges for the Host Checker to enforce the connection control policy on the client computer.

To enable the predefined Host Checker connection control policy:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to enable the predefined Host Checker connection control policy.
2. Click the **Configuration** tab, and select **Authentication > Endpoint Security > Host Checker**.
3. Select **Settings > Options**, and then select the **Perform dynamic policy reevaluation** check box.
4. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.



NOTE: You must evaluate or enforce the connection control policy at the realm level to make the policy effective on client computers.

Related Documentation

- [Enabling Predefined Client-Side Policies for Windows Only \(NSM Procedure\) on page 247](#)
- [Configuring Virus Signature Version Monitoring \(NSM Procedure\) on page 248](#)

Configuring Virus Signature Version Monitoring (NSM Procedure)

You can configure Host Checker to monitor and verify that the virus signatures, operating systems, software versions, and patches installed on client computers are up to date, and remediate those endpoints that do not meet the specified criteria. Host Checker uses the current virus signatures and patch assessment versions from the vendor(s) you specify for predefined rules in a Host Checker policy.

You can automatically import either the current Virus signature version monitoring or Patch Management Info Monitoring list from the Juniper Networks staging site at a specified interval. Alternatively, you can download the files from Juniper Networks and use your own staging server.

You can also configure a proxy server as a staging site between the device and the Juniper Networks site. To use a proxy server, you must enter the servers network address, and port and authentication credentials, if applicable.

To configure the device to automatically import the current virus signature version monitoring:

1. In the navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure the device to automatically import the current signature version monitoring.
2. Click the **Configuration** tab and select **Authentication > Endpoint Security > Host Checker**.
3. Click either **Virus signature version monitoring** or **Patch Management Info Monitoring**.
4. Select either **Auto-update virus signatures list** or **Auto-update Patch Management data**.
5. Configure the device to automatically import the current signature version monitoring using the settings described in [Table 68 on page 248](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 68: Configuring Virus Signature Version Monitoring Details

Options	Your Action
Download path	Specifies the existing URLs of the staging sites where the current lists are stored. The default URLs are the paths to the Juniper Networks staging site: https://download.juniper.net/software/av/uac/epupdate_hist.xml (for auto-update virus signatures list).
Download interval	Specifies how often you want the device to automatically import the current list(s).
Username	Enter your Juniper Networks Support username.
Password	Enter your Juniper Networks Support password.

- Related Documentation**
- [Importing Virus Signature Version Monitoring or Patch Management Version Monitoring List \(NSM Procedure\) on page 249](#)
 - [Assigning a Proxy Server an Auto-Update Server \(NSM Procedure\) on page 249](#)

Importing Virus Signature Version Monitoring or Patch Management Version Monitoring List (NSM Procedure)

To manually import either the current virus signature version monitoring or the patch management version monitoring list:

1. In the navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to import either the virus signature version monitoring or the patch management version monitoring list.
2. Click the **Configuration** tab and select **Authentication > Endpoint Security > Host Checker**.
3. Click either **Virus signature version monitoring** or **Patch Management Info Monitoring**.
4. Download the list from the Juniper Networks staging site to a network server or local drive on your computer by entering the Juniper Networks URLs in a browser window.
https://download.juniper.net/software/av/uac/epupdate_hist.xml
<https://download.juniper.net/software/hc/patchdata/patchupdate.dat>
5. Under Manually import virus signatures list, click **Browse**, select the list, and then click **OK**.
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.



NOTE: If you use your own staging site for storing the current list, you must upload the trusted root certificate of the CA that signed the staging's server certificate to the device.

- Related Documentation**
- [Configuring Virus Signature Version Monitoring \(NSM Procedure\) on page 248](#)
 - [Assigning a Proxy Server an Auto-Update Server \(NSM Procedure\) on page 249](#)

Assigning a Proxy Server an Auto-Update Server (NSM Procedure)

To use a proxy server as an auto-update server:

1. In the navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to use the proxy server as an auto-update server.
2. Click the **Configuration** tab and select **Authentication > Endpoint Security > Host Checker**.

3. Click either **Virus signature version monitoring** or **Patch Management Info Monitoring**.
4. Select either **Auto-update virus signatures list** or **Auto-update Patch Management data**.
5. Configure settings as described in [Table 69 on page 250](#).
6. If your proxy server is password protected, type the username and password of the proxy server.
7. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 69: Proxy Server as Auto-Update Server details

Options	Your Action
Download path	Specifies the existing URLs of the staging sites where the current lists are stored. The default URLs are the paths to the Juniper Networks staging site: https://download.juniper.net/software/av/uac/epupdate_hist.xml https://download.juniper.net/software/hc/patchdata/patchupdate.dat
Download interval	Specifies how often you want the device to automatically import the current list(s).
Username and Password	Enter your Juniper Networks Support credentials.
Use Proxy Server	Select the check box to enable this feature.
IP Address	Enter the IP address of your proxy server.
Port	Enter the port that the Juniper Networks Support site will use to communicate with your proxy server.

- Related Documentation**
- [Configuring Virus Signature Version Monitoring \(NSM Procedure\) on page 248](#)
 - [Importing Virus Signature Version Monitoring or Patch Management Version Monitoring List \(NSM Procedure\) on page 249](#)

Configuring Secure Access Cache Cleaner

- [Configuring Global Cache Cleaner Options \(NSM Procedure\) on page 251](#)
- [Configuring Cache Cleaner Restrictions \(NSM Procedure\) on page 254](#)

Configuring Global Cache Cleaner Options (NSM Procedure)

Cache Cleaner is a Windows client-side agent that removes residual data, such as temporary files or application caches, left on a user's machine after a Secure Access session. When you enable Cache Cleaner, it clears all content downloaded through the Secure Access devices Content Intermediation Engine from a user's system.

To configure global Cache Cleaner options:

1. In the navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure global Cache Cleaner options.
3. Click the **Configuration** tab and select **Authentication > Endpoint Security > Cache Cleaner**. The corresponding workspace appears.
4. Configure the global Cache Cleaner options using the settings described in [Table 70 on page 251](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 70: Configuring Global Cache Cleaner Details

Option	Function	Your Action
Cache Cleaner > General tab		
Cleaner Frequency (minutes)	Specifies how often Cache Cleaner is to run. Each time Cache Cleaner must run, it clears all content downloaded through the Secure Access device's Content Intermediation Engine plus the browser cache, files, and folders you specify under the Browser Cache and Files and Folders sections.	Enter the time in minutes. NOTE: Valid values range from 1 to 60 minutes.

Table 70: Configuring Global Cache Cleaner Details (*continued*)

Option	Function	Your Action
Status Update Frequency (minutes)	Specifies how often the Secure Access device expects the Cache Cleaner to update the status.	Enter the time in minutes. NOTE: Valid values range from 1 to 60 minutes.
Client-side process, login inactivity timeout (minutes)	Specifies an interval to control timing out.	Enter the time in minutes. NOTE: Valid values range from 5 to 60 minutes.
Disable AutoComplete of web addresses	Allows you to prevent the browser from using cached values to automatically fill in Web addresses during the user's Secure Access device session.	Select the Disable AutoComplete of web addresses check box to enable this feature.
Disable AutoComplete of usernames and passwords	Allows you to prevent Internet Explorer from automatically filling in user credentials in Web forms using cached values. Selecting this option also disables the "Save Password?" prompt on Windows systems.	Select the Disable AutoComplete of usernames and passwords check box to enable this feature.
Flush all existing AutoComplete passwords	Clears any cached passwords that Internet Explorer has cached on the user's system.	Select the Flush all existing AutoComplete passwords check box to enable this feature.
Flush all existing AutoComplete passwords:	Allows Secure Access device to restore the user's cached passwords at the end of the user Secure Access device session or to permanently delete the user's cached passwords.	Select one of the following options from the drop-down list: <ul style="list-style-type: none"> • For the IVE session only—Secure Access device restores the user's cached passwords at the end of his Secure Access device session. • Permanently—Permanently deletes the user's cached passwords.
Empty Recycle Bin and Recent Documents list at the end of user session	Allows you to empty the recycle bin and clear the recent documents list. The entire contents are removed, not just the files related to the user's sessions.	Select the Empty Recycle Bin and Recent Documents list at the end of user session check box to enable this feature.
Uninstall Cache Cleaner at logout	Allows you to enable Secure Access device to uninstall Cache Cleaner from the client machine when a user's session ends.	Select the General tab > Uninstall Cache Cleaner at logout check box to enable this feature.
Cache Cleaner > Browser Cache tab		
Hostname	Allows you to enter one or more hostnames or domains (wildcards are permitted).	Enter the hostname or domain.

Table 70: Configuring Global Cache Cleaner Details (*continued*)

Option	Function	Your Action
Cache Cleaner > Files and Folders		
Clear folders only at the end of session	Enables Cache Cleaner to clear directory contents only at the end of the user session. Otherwise, Cache Cleaner also clears files and folders at the specified cleaner frequency interval.	Select the Clear folders only at the end of session check box to enable this feature.
File or folder path	Specifies the name of a file that you want Cache Cleaner to remove.	Enter the name of the file.
Clear Subfolders	Enables Cache Cleaner also to clear the contents of any subdirectories within this directory.	Select the Files and Folders > Clear Subfolders check box to enable this feature.

Related Documentation

- [Configuring Cache Cleaner Restrictions \(NSM Procedure\) on page 254](#)
- [Configuring the Network Communications Protocol \(NSM Procedure\) on page 257](#)

Configuring Cache Cleaner Restrictions (NSM Procedure)

You can restrict Secure Access device and resource access by requiring Cache Cleaner in the following options:

- **Realm authentication policy**—When users try to sign in to the Secure Access device, the Secure Access device evaluates the specified realm's authentication policy to determine if the preauthentication requirements include Cache Cleaner. You can configure a realm authentication policy to download Cache Cleaner, download and start running Cache Cleaner, or not require Cache Cleaner. The user must sign in using a computer that adheres to the Cache Cleaner requirements specified for the realm. If the user's computer does not meet the requirements, then the user is denied access to the Secure Access device.
- **Role**—When the Secure Access device determines the list of eligible roles to which it can map an administrator or user, it evaluates each role's restrictions to determine if the role requires Cache Cleaner to run on the user's workstation. If it does and the user's machine is not already running Cache Cleaner, then the Secure Access device does not map the user to that role.
- **Resource policy**—When a user requests a resource, the Secure Access device evaluates the resource policy's detailed rules to determine whether or not Cache Cleaner needs to be installed or running on the user's workstation. The Secure Access device denies access to the resource if the user's machine does not meet the Cache Cleaner requirement.
-

To configure Cache Cleaner restrictions at the realm level:

1. In the navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure global Cache Cleaner restrictions in realm level.
3. Click the **Configuration** tab and select **Users > User Realms > Select Realm > Authentication Policies > Cache Cleaner**. The corresponding workspace appears.
4. Configure the cache cleaner restrictions at the role level using the settings described in [Table 71 on page 254](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 71: Configuring Cache Cleaner Restrictions Details at Realm Level

Option	Function	Your Action
Files and Folders		

Table 71: Configuring Cache Cleaner Restrictions Details at Realm Level (continued)

Option	Function	Your Action
Cache Cleaner option	Specifies whether or not Cache Cleaner is running for the user to meet the access requirement.	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • Disable Cache Cleaner—Does not require Cache Cleaner to be installed or running for the user to meet the access requirement. • Just load Cache Cleaner (Loads after IVE maps the user to a realm)—Does not require Cache Cleaner to be running for the user to meet the access requirement but ensures that it is available for future use. If you choose this option for a realm's authentication policy, then the Secure Access device downloads Cache Cleaner to the client machine after the user is authenticated and before the user is mapped to any roles on the system. • Load and enforce Cache Cleaner (Loads before IVE maps the user to a realm)—Requires the Secure Access device to download and run Cache Cleaner for the user to meet the access requirement. If you choose this option for a realm's authentication policy, then the Secure Access device downloads Cache Cleaner to the client machine before the user may access the Secure Access device sign-in page.

To configure cache cleaner restrictions at the role level:

1. In the navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure global Cache Cleaner restrictions at the role level.
3. Click the **Configuration** tab and select **Users > User Roles > Select Role > General > Restrictions > Cache Cleaner Restrictions**. The corresponding workspace appears.
4. Configure the Cache Cleaner restrictions at the role level using the settings described in [Table 72 on page 255](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 72: Configuring Cache Cleaner Restriction Details at role level

Option	Function	Your Action
Require Cache Cleaner (must be loaded by the Realm)	Specifies Cache Cleaner to be running in order for the user to meet the access requirement.	Select the Require Cache Cleaner (must be loader by the Realm) check box to enable this option.

To configure Cache Cleaner restrictions at the resource policy level:

1. In the navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure global Cache Cleaner restrictions at the resource policy level.

3. Click the **Configuration** tab and select **Users > Resource Policies > Select Resource > Select Policy > Detailed Rules**.
4. Select or create the rule and configure the Cache Cleaner restrictions at the resource policy level using the settings described in [Table 73 on page 256](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 73: Configuring Global Cache Cleaner Restriction Detail at Resource Policy Level

Option	Function	Your Action
General tab		
Name	Specifies the resource policy's detailed rule name.	Enter the name.
Action	Specifies the action to allow the Secure Access device to access the resource if the user's machine does not meet the Cache Cleaner requirement.	Select Allow or Deny from the drop-down list.
Resources	Specifies the resource or a partial list of the resources.	Enter specific URL, directory path, file, or file type.
Conditions	Specifies a custom expression in a detailed rule for the Secure Access device to determine whether or not Cache Cleaner needs to be installed or running on the user's workstation.	Enter the custom expression.

Related Documentation

- [Configuring the Network Communications Protocol \(NSM Procedure\) on page 257](#)
- [Configuring Global Cache Cleaner Options \(NSM Procedure\) on page 251](#)

Configuring Secure Access System Management Features

- [Configuring the Network Communications Protocol \(NSM Procedure\) on page 257](#)
- [Configuring Secure Meetings \(NSM Procedure\) on page 259](#)
- [Configuring Global Security \(NSM Procedure\) on page 261](#)
- [Configuring Sensors \(NSM Procedure\) on page 265](#)
- [Creating a Custom Expression for Sensor Settings \(NSM Procedure\) on page 268](#)

Configuring the Network Communications Protocol (NSM Procedure)

The Network Communications Protocol is used to communicate between the Secure Access device server and client applications.

To configure the Network Communications Protocol:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure network communications protocol.
2. Click the **Configuration** tab, and select **System > Configuration > NCP**. The corresponding workspace appears.
3. Add or modify settings as specified in [Table 74 on page 258](#).
4. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modification.

Table 74: Configuring Network Communications Protocol Details

Option	Function	Your Action
NCP Auto-Select	Allows you to specify internal protocols to communicate between the Secure Access device server and client applications.	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • Auto-select enabled— Secure Access device uses NCP for most client/server communications and then switches to standard NCP when necessary. • Auto-select disabled—Secure Access device uses standard NCP for client/server communications. This option is primarily provided for backwards compatibility.
Read Connection Timeout (seconds)	Allows you to specify the timeout interval for Java clients (15 to 120 seconds). Note that this value does not apply to user inactivity in client applications.	Set the idle connection interval.
Idle Connection Timeout (minutes)	Allows you to specify the idle connection interval. This timeout interval determines how long the Secure Access device maintains idle connections for client-side Windows Secure Access methods.	Set the idle connection interval.

Related Documentation

- [Configuring General Network Settings \(NSM Procedure\) on page 271](#)
- [Configuring Internet Protocol Filters \(NSM Procedure\) on page 276](#)

Configuring Secure Meetings (NSM Procedure)

Unlike other access features, Secure Meeting does not have a resource policy. Instead, you configure system-level settings that apply to all roles for which this feature is enabled. You can:

- Specify session lifetime limits for meetings.
- Enable daylight savings adjustments to scheduled meetings.
- Specify the maximum color depth of meeting presentations.
- Enable automatic email notifications for users who are invited to meetings scheduled through the Secure Access device end user console.
- Define the MySecureMeeting URL.

To configure secure meetings:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure secure meetings.
2. Click the **Configuration** tab, and select **System > Configuration > Secure Meeting**. The corresponding workspace appears.
3. Add or modify settings as specified in [Table 75 on page 259](#).
4. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modification.

Table 75: Configuring Secure Meeting Details

Option	Function	Your Action
Idle Timeout (minutes)	Specifies the number of minutes a meeting session may remain idle before ending.	Enter the time.
Max. Session Length (minutes)	Specifies the number of minutes a meeting session may remain open before ending.	Enter the time.
Enable Upload Logs	Allows non-Secure Access device users to upload meeting logs.	<p>Select Enable Upload Logs to enable this feature.</p> <p>NOTE: If you select the Upload Logs option, you must also use settings in the System > Log/Monitoring > Client Logs > Settings page of the admin console to enable client-side logging.</p>

Table 75: Configuring Secure Meeting Details (*continued*)

Option	Function	Your Action
Root meeting URL	<p>Allows you to select the meeting URL you want to associate with MySecureMeeting meetings.</p> <p>NOTE: Meeting URLs are created in the Authentication > Signing In > Sign-In Policies page.</p>	Select the meeting URL.
Meeting name	<p>Specifies the token to append to the meeting URL to uniquely identify this URL.</p>	<p>Select any one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • Username—Appends the user's Secure Access device username to the meeting URL. • Sequential room number with prefix—Specifies a string to append to the meeting URL, such as a "meeting". Numbers will be appended to the string to ensure uniqueness. • Expression—Appends an expression, such as <code><userAttr.lname></code>, to the meeting URL. If the attribute is not valid, username is appended to the meeting URL instead.
Meeting room number prefix	<p>Allows you to specify a string to append to the meeting URL, such as a "meeting". Numbers will be appended to the string to ensure uniqueness</p> <p>For example, meeting_room1, meeting_room2.</p>	Specify a string.
Meeting name expression	<p>Allows you to specify an expression, such as <code><userAttr.lname></code>, to the meeting URL. If the attribute is not valid, username is appended to the meeting URL instead.</p>	Specify an expression.
SMTP Server	<p>Allows you to specify the IP address or host name of the SMTP server that can route email traffic from the appliance to the meeting invitees.</p>	Enter the IP address or host name of the SMTP server.
SMTP Login	<p>Allows you to specify a valid login name for the specified SMTP email server (if required by the SMTP server).</p>	Enter a valid login name for the SMTP email server.
SMTP Password (clear text)	<p>Allows you to specify a password for the specified SMTP email server.</p>	Enter the password for the specified SMTP email server.
SMTP Email	<p>Specifies the email address or the address of another administrator that secure meeting uses the specified address as the sender's email if the email creator does not configure his own email address on the Secure Access device.</p>	Enter the email address or the address of another administrator.

Table 75: Configuring Secure Meeting Details (*continued*)

Option	Function	Your Action
Observe DST schedules of this country	Allows you to specify the country whose daylight savings time rules the Secure Access device should observe. The client uses this setting as a baseline and then adjusts meeting times for individual users as necessary based on browser settings and Secure Access device client-side DST preference settings.	Select a country from the drop down list.
Enable 32-bit (True Color) Presentations	Allows users to present in true color. By default, Secure Meeting presents applications to users using the same color-depth as the presenter's desktop (up to 32-bit color). If you do not select this option and a user presents an application in 32-bit color, however, Secure Meeting changes the image to 16-bit to improve performance.	Select Enable 32-bit (True Color) Presentations to enable this feature.

- Related Documentation**
- [Configuring Global Security \(NSM Procedure\) on page 261](#)
 - [Configuring Sensors \(NSM Procedure\) on page 265](#)

Configuring Global Security (NSM Procedure)

The default global security settings provide maximum security. However, you may need to modify these settings if users cannot use certain browsers or access certain web pages. You can also configure lockout options for protecting the Secure Access device and back-end systems from DoS/DDoS/password guessing attacks from the same IP address.

To configure global security:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure global security.
2. Click the **Configuration** tab, and select **System > Configuration > Global Security**. The corresponding workspace appears.
3. Add or modify settings as specified in [Table 76 on page 261](#).
4. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modification.

Table 76: Configuring Global Security Details

Option	Function	Your Action
SSL Settings > General tab		

Table 76: Configuring Global Security Details (*continued*)

Option	Function	Your Action
Allowed SSL and TLS Version	Specifies encryption requirements for Secure Access device users.	<p>Select any one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • Accept only TLS V1 (maximize security with reduced compatibility)—For maximize security with reduced compatibility. • Accept only SSL V3 and TLS V1 (maximize security)—For maximize security. • Accept SSL V2 and V3 and TLS V1 (maximize browser compatibility)—For users who have older browsers that use SSL version 2 to update their browsers or change the Secure Access device setting to allow SSL version 2, SSL version 3, and TLS. <p>NOTE: The Secure Access device requires SSL version 3 and TLS by default.</p>
strength	Specifies the encryption strength.	<p>Select one of the following options from the drop-down list.</p> <ul style="list-style-type: none"> • Accept only 168-bit and greater (maximize security)—Secure Access device gives preference to 256-bit AES over 3DES • Accept only 128-bit and greater (security and browser compatibility)—Secure Access device gives preference to RC4 ciphers. • Accept 40-bit and greater (maximize browser compatibility)—Secure Access device gives preference to RC4 ciphers. • Custom SSL Cipher Selection—Specifies a combination of cipher suites for the incoming connection from the user's browser.
AES/3DES High (168-bit and greater)	<p>Allows the Secure Access device to provide preference to 256-bit AES over 3DES.</p> <p>NOTE: This option is displayed only when you select Custom SSL Cipher Selection from the strength drop-down list.</p>	Select the AES/3DES High (168-bit and greater) check box to enable this feature.

Table 76: Configuring Global Security Details (*continued*)

Option	Function	Your Action
AES Medium (between 128-bit and 168-bit)	Allows the Secure Access device to use 168-bit or higher ciphers for backend rewriter connections and the device to provide preference to 256-bit AES encryption for backend mail proxy SSL connections. NOTE: This option is displayed only when you select Custom SSL Cipher Selection from the strength drop-down list.	Select the AES Medium (between 128-bit and 168-bit) check box to enable this feature.
RC4 Medium (between 128-bit and 168-bit)	Allows Secure Access device to use 168-bit or higher ciphers for backend rewriter connections and the device provides preference to 256-bit AES encryption for backend mail proxy SSL connections. NOTE: This option is displayed only when you select Custom SSL Cipher Selection from the strength drop-down list.	Select the RC4 Medium (between 128-bit and 168-bit) check box to enable this feature.
RC2 Medium (between 128-bit and 168-bit)	Allows Secure Access device to use 168-bit or higher ciphers for backend rewriter connections and device gives preference to 256-bit AES encryption for backend mail proxy SSL connections. NOTE: This option is displayed only when you select Custom SSL Cipher Selection from the strength drop-down list.	Select the RC2 Medium (between 128-bit and 168-bit) check box to enable this feature.
DES Low (less than 128-bit)	Allows Secure Access device to use 168-bit or higher ciphers for backend rewriter connections and the device provides preference to 256-bit AES encryption for backend mail proxy SSL connections. NOTE: This option is displayed only when you select Custom SSL Cipher Selection from the strength drop-down list.	Select the DES Low (less than 128-bit) check box to enable this feature.
Do not allow connections from browsers that only accept weaker ciphers	Prevents a browser with a weak cipher from establishing a connection.	Select the Do not allow connections from browsers that only accept weaker ciphers check box to enable this feature.

Settings

Table 76: Configuring Global Security Details (*continued*)

Option	Function	Your Action
Lockout period (minutes)	Specifies the number of minutes you want the Secure Access device to lock out the IP address.	Enter the time.
Attempts	Specifies the maximum number of failed sign-in attempts to allow before triggering the initial lockout.	Enter the number of attempts.
Rate	Specifies the number of failed sign-in attempts to allow per minute.	Enter the number of sign-in attempts to allow per minute.
Show last login time on user's bookmark page	Displays the day and time the user last logged in to the system in the bookmark page.	Select the Show last login time on user's bookmark page check box to enable this feature.
Show last login IP address on user's bookmark page	Displays the IP address when user last logged in to the system in the bookmark page.	Select the Show last login IP address on user's bookmark page check box to enable this feature.
Delete all cookies at session termination	Allows Secure Access device to set persistent cookies on the user's machine to support functions such as multiple sign-in, last associated realm, and last sign-in URL. If you desire additional security or privacy, you may choose to not set them.	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • Delete all cookies at session termination (maximize security)—Secure Access device deletes all cookies at session termination. • Preserve cookies at session termination—Secure Access device preserves cookies at session termination.
Include IVE's session cookie in URL	Allows Secure Access device to include the user session cookie in the URL that launches JSAM or a Java applet. By default, this option is enabled, but if you have concerns about exposing the cookie in the URL, you can disable this feature.	<p>Select any one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • Include session cookie in URL (maximize compatibility)—Secure Access device includes session cookie in URL. • Do not include session cookie in URL (maximize security)—Secure Access device does not include the session cookie in URL.
SAML version	Allows you to specify the SAML protocol and schema.	Select SAML 1.0 or SAML 1.1 from the drop-down list.

Related Documentation

- [Configuring Sensors \(NSM Procedure\) on page 265](#)
- [Configuring the Network Communications Protocol \(NSM Procedure\) on page 257](#)

Configuring Sensors (NSM Procedure)

The IDP sensor is a powerful tool to counter users who initiate attacks. Integration with the Secure Access device allows you to configure automatic responses as well as manually monitor and manage users.

To configure IDP sensors:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure sensors.
2. Click the **Configuration** tab, and select **System > Configuration > Sensors**. The corresponding workspace appears.
3. Add or modify settings as specified in [Table 77 on page 265](#).
4. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modification.

Table 77: Configuring IDP Sensor Details

Option	Function	Your Action
Sensors tab		
Name	Specifies the name that the Secure Access device uses to identify the new connection entry.	Enter the name.
Hostname	Specifies the hostname or IP address of the IDP sensor to which the Secure Access device connects to receive application and resource attack alert messages.	Enter the hostname or IP address.
TCP Port	Specifies the TCP port on the IDP sensor to which the Secure Access device listens when receiving application and resource attack alert messages.	Enter the port.
One Time Password	Specifies the encrypted password the Secure Access device uses when conducting the initial Transport Layer Security (TLS) handshake with the IDP sensor.	Enter the encrypted Secure Access device OTP password as displayed on the IDP ACM configuration summary screen.
Addresses to monitor > New Addresses to monitor	Allows you to specify individual IP addresses and address ranges the IDP sensor monitors for potential attacks, one entry per line. IDP reports attack information only for the IP addresses that you specify.	Enter the IP addresses.

Table 77: Configuring IDP Sensor Details (*continued*)

Option	Function	Your Action
Severity Filter	Specifies the severity level from 1 to 5, where 1 is informational and 5 is critical.	Select one of the options available from the drop-down list.
Enable/Disable Sensor	Enables the specified IDP sensor entries, respectively.	Select the Enable/Disable Sensor check box to enable this feature.
Sensor Event Policies tab		
Name	Specifies the rule name of the action(s) the Secure Access device takes when it receives attack alert messages from an IDP sensor.	Enter the rule name.
Event	Allows you to specify an event.	Select an event from the drop-down list.
Event Count	Determines the number of times an event must occur before action is taken.	Enter a number between 1 and 256 to determine the number of times an event must occur before action is taken.
Action to be taken	Allows you to specify the action(s) the Secure Access device takes when it receives attack alert messages from an IDP sensor.	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • Ignore (just log the event)— Secure Access device logs the event, and takes no further action against the user profile to which this rule applies. • Terminate user session— Secure Access device immediately terminates the user session and requires the user to sign in to the Secure Access device again. • Disable user account—Secure Access device disables the user profile associated with this attack alert message, thus rendering the client unable to sign in to the Secure Access device until the administrator reenables the user account. (This option is only applicable for users who have a local Secure Access device user account.) • Replace user role—Specifies that the role applied to this user's profile should change to the role you select from the associated drop-down list. This new role remains assigned to the user profile until the session terminates.

Table 77: Configuring IDP Sensor Details (*continued*)

Option	Function	Your Action
Replace user role with this role	<p>Allows you to change the user role applied to this user's profile with this role.</p> <p>NOTE: This option is enabled only when you select Replace user role from the Action to be taken drop-down list.</p>	Select a role from the drop-down list.
Replace user role..	<p>Allows you to make this role assignment.</p> <p>NOTE: This option is enabled only when you select Replace user role from the Action to be taken drop-down list.</p>	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • Permanent—User remains in the quarantined state across subsequent logins until the administrator releases the user from the quarantined state. • For this session only—Default. User can log in to another session.
Applies to Roles	Allows you to apply this policy to all roles or only to the users mapped or only to the users who are not mapped to roles.	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • All—Applies this policy to all users. • Selected—Applies this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list. • Except those selected—Applies this policy to all users except for those who are mapped to the roles in the members list. Make sure to add roles to this list from the Available roles list.
Role Selection	Allows you to select and map roles to user.	Select a role and click Add .
Sensor Events tab		
Name	Specify a name for the event.	Enter the name.
Expressions	Specifies the expressions.	<p>Enter the expressions or select one or more clauses from the expressions dictionary and click insert expression.</p> <p>For example, to check for all critical/highest severity level attacks, enter the following expression: idp.severity >= 4</p>

Related Documentation

- [Configuring General Network Settings \(NSM Procedure\) on page 271](#)
- [Configuring Global Security \(NSM Procedure\) on page 261](#)

Creating a Custom Expression for Sensor Settings (NSM Procedure)

Custom expressions are strings that are made up of variables, operators, and sub expressions all concatenated together. These operators and variables are provided through an expressions dictionary.

To create a custom expression for sensor settings:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure sensor settings.
3. Click the **Configuration** tab. In the configuration tree, select **System > Configuration > Sensors**.
4. Select the **Sensor Events** tab.
5. Click **New** to create a custom expression. The Custom Expression editor appears. On the left side of the editor is the Expression Dictionary, which includes the following custom expression building blocks:
 - **Logical Operators:** This node consists of logical operators that are used to build expressions. Select a logical operator and click the **Insert Expression** button to insert logical operators in expressions.
 - **Prebuilt Expressions:** This node consists of expressions that function as templates for custom expressions. Select a prebuilt expression and click the **Insert Expression** button. The prebuilt expression is displayed in the Expression area. Modify the values to create your own custom expression.
 - **Variables:** This node consists of variables. When a variable is selected, the conditional operators that can be applied to this variable are listed in the center of the Custom Expressions editor. Also, some variables have extensions that are displayed in the drop-down list next to the variable. Double-click a variable to display its description and example usage. Click the example variable to insert it in the Expression area.
 - **IF-MAP Variables:** This node consists of IF-MAP variables. Double-click a IF-MAP variable to display its description and example usage. Click the IF-MAP variable example to insert it in the Expression area.
 - **Juniper IDP Variables:** This node consists of Juniper IDP variables. Double-click a Juniper IDP variable to display its description and example usage. Click the Juniper IDP variable example displayed to insert it in the Expression area.



NOTE: Refer to the *Juniper Networks Secure Access Administration Guide* for more information on variables and writing custom expressions.

6. Enter a name for the custom expression.
7. Select a variable or prebuilt expression from the Custom Dictionary, and click **Insert Expression**. The expression is displayed in the Expression area on the right side of the

Custom Expression editor. The conditional operators can be selected only after a leaf node is selected.

8. Click the **Validate** button to validate the expression. The expression is validated by the device and the validation status appears.



NOTE: You can create a custom expression in a device template, but you cannot validate the custom expression. The Validate button is not enabled in the Custom Expressions editor of device templates.

9. Click **OK** to save the custom expression. The new custom expression is displayed under the Sensor Events tab.
10. Click **OK** to save the sensor events settings.

**Related
Documentation**

- [Configuring Sensors \(NSM Procedure\) on page 265](#)
- [Configuring User Access, Admin Access, Events and Sensors \(NSM Procedure\) on page 305](#)

Configuring Network Settings

- [Configuring General Network Settings \(NSM Procedure\) on page 271](#)
- [Configuring Internal Ports \(NSM Procedure\) on page 273](#)
- [Configuring Hosts \(NSM Procedure\) on page 275](#)
- [Configuring Internet Protocol Filters \(NSM Procedure\) on page 276](#)

Configuring General Network Settings (NSM Procedure)

Configuring general network settings in NSM enables you to view the status of the system ports, specifies a host name for the Secure Access device, and configures DNS name resolution, Windows Internet Naming Service (WINS) server, and master browser settings for the Secure Access device.

To configure general network settings:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure general network settings.
2. Click the **Configuration** tab, and select **System > Network Settings > Overview** tab. The corresponding workspace appears.
3. Add or modify settings as specified in [Table 78 on page 271](#).
4. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modification.

Table 78: Configuring General Network Settings Details

Option	Function	Your Action
General Settings tab		
Hostname for network identity	Specifies the fully-qualified host name of the Secure Access device for network identity.	Enter the name of the Secure Access device. NOTE: You can enter upto maximum of 30 characters as host name.

Table 78: Configuring General Network Settings Details (*continued*)

Option	Function	Your Action
Primary DNS	Specifies the primary DNS IP address.	Enter the primary DNS IP address.
Secondary DNS	Specifies the secondary DNS IP address.	Enter the primary DNS IP address.
New DNS Domain(s)	Allows you to specify the default DNS domain name for the individual Secure Access device appliance.	Enter a comma delimited list of DNS domains; The Secure Access device searches for them in the order that they are listed.
WINS	Allows you to specify the name or IP address of a local or remote Windows Internet Naming Service (WINS) server that you use to associate workstation names and locations with IP addresses (if applicable).	Enter the name or IP address of a local or remote WINS.
Windows networking tab		
Enable network discovery (allows detection of Windows share folders)	Enables the Secure Access device to discover shared Windows folders.	Select Windows networking tab > Enable network discovery (allows detection of Windows share folders) to enable this option.
Master Browsers > Name	Allows you to select a WINS server, domain controller, or other server within the Secure Access device domain that responds to NETBIOS calls and associates workstation names and locations with IP addresses (if applicable).	Enter the master browser name.

Related Documentation

- [Configuring Internal Ports \(NSM Procedure\) on page 273](#)
- [Configuring Hosts \(NSM Procedure\) on page 275](#)

Configuring Internal Ports (NSM Procedure)

The internal port, also known as the internal interface, handles all LAN requests to resources, listening for Web browsing, file browsing, authentication, and outbound mail requests.

To configure internal port settings:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure internal ports.
2. Click the **Configuration** tab, and select **System > Network Settings > Internal Port** tab. The corresponding workspace appears.
3. Add or modify settings as specified in [Table 79 on page 273](#).
4. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modification.

Table 79: Configuring Internal Port Details

Option	Function	Your Action
General tab		
IP Address	Specifies the IP address for the individual Secure Access device. By default, these boxes are populated with the settings entered during initial Secure Access device setup.	Enter the IP address.
Netmask	Specifies the netmask for the individual Secure Access device. By default, these boxes are populated with the settings entered during initial Secure Access device setup.	Enter the netmask.
Default Gateway	Specifies the default gateway settings for the individual Secure Access device. By default, these boxes are populated with the settings entered during initial Secure Access device setup.	Enter the IP address for the default gateway.
Link Speed	Allows you to specify the speed and duplex combination you want to use for the internal port.	Select the link speed from the drop-down list.
ARP Ping Timeout (seconds)	Specifies how long the Secure Access device should wait for responses to Address Resolution Protocol (ARP) requests before timing out.	Enter the time in seconds.

Table 79: Configuring Internal Port Details (*continued*)

Option	Function	Your Action
MTU (bytes)	Specifies a maximum transmission unit for the Secure Access device's internal interface.	Enter the unit in bytes. NOTE: Use the default MTU setting (1500) unless you must change the setting for troubleshooting purposes.
Routes > Destination Network/IP	Allows you to specify the destination network/IP address.	Enter the name/IP address for the destination network.
Routes > Netmask	Specifies the netmask of the static route that the Secure Access device should use when routing requests.	Enter the netmask of the static route.
Routes > Gateway	Specifies the gateway of the static route that the Secure Access device should use when routing requests.	Enter the IP address of the gateway of the static route.
Routes > Interface	Specifies the interface of the static route that the Secure Access device should use when routing requests.	Enter the IP address of the interface of the static route.
Routes > Metric	Specifies metric for comparing multiple routes to establish precedence. NOTE: Generally, the lower the number, from 1 to 15, the higher the precedence. So, a route with a metric of 2 would be chosen over a route with a metric of 14. The metric value of zero (0) identifies the route as one that should not be used.	Enter the metric.
Virtual Ports tab		
Name	Specifies a unique name for the virtual port.	Enter the name.
IP Address	Specifies a unique IP alias to associate with the virtual port. NOTE: Do not use an IP address that is already associated with another virtual port.	Enter the IP address.
ARP Cache tab		
IP Address	Specifies the IP address of a network device such as a router or backend application server that connects to the Secure Access device to determine the physical (MAC) address.	Enter the IP address.
Physical Address	Specifies the physical address of a network device such as a router or backend application server that connects to the Secure Access device to determine the physical (MAC) address	Enter the physical address.

- Related Documentation
- [Configuring Hosts \(NSM Procedure\) on page 275](#)
 - [Configuring Internet Protocol Filters \(NSM Procedure\) on page 276](#)

Configuring Hosts (NSM Procedure)

You can configure hostnames in NSM that the Secure Access device can resolve to IP addresses. This feature is useful when:

- Your DNS server is not accessible to the Secure Access device.
- You use WINS to access servers within the LAN.
- Your corporate security policy does not allow internal servers to be listed on an external DNS or requires that internal hostnames are masked.

To configure hosts:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure hosts.
2. Click the **Configuration** tab, and select **System > Network Settings > Hosts**. The corresponding workspace appears.
3. Add or modify settings as specified in [Table 80 on page 275](#).
4. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modification.

Table 80: Configuring Host Details

Option	Function	Your Action
Settings tab		
IP	Specifies the IP address of the hostname.	Enter the IP address.
Name(S)	Specifies the hostnames that the Secure Access device can resolve to the IP address.	Enter a comma delimited list of hostnames.
Comment	Allows you to enter a comment of 200 words or less (optional).	Enter the comment.

- Related Documentation
- [Configuring Internet Protocol Filters \(NSM Procedure\) on page 276](#)

Configuring Internet Protocol Filters (NSM Procedure)

You can configure IP filters in NSM that the Secure Access device can apply to Network Connect IP pools.

To configure Internet protocol filters:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure Internet protocol filters.
2. Click the **Configuration** tab, and select **System > Network Settings > Network Connect**. The corresponding workspace appears.
3. Add or modify settings as specified in [Table 81 on page 276](#).
4. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modification.

Table 81: Configuring Internet Protocol Filters Details

Option	Function	Your Action
Settings tab		
NC Base IP Address	Displays the default Network Connect IP address.	Only change the Network Connect server IP address when instructed to do so by the Juniper Networks support team.
IP Address Filters	Specifies the IP address filters.	Enter the IP address filter.

Related Documentation

- [Managing Large Binary Data Files \(NSM Procedure\) on page 295](#)
- [Configuring General Network Settings \(NSM Procedure\) on page 271](#)

CHAPTER 19

Synchronizing User Records

User record synchronization relies on client/server pairings. The client is the Secure Access appliance that users log in to start their remote access. Each client is associated with one primary server and one backup server to store user record data. Clients can be individual appliances or a node within a cluster.

A server in this instance is the Secure Access appliance that stores the user record data. Each server can be configured to replicate its user record data to one or more peer servers. Servers are identified by a user-defined logical name. The same logical name can be assigned to more than one authentication server to let you associate authentication servers of different types to the same user. For example, SA1 is an ACE authentication server with user1 who creates a bookmark to www.juniper.net. SA2 is an Active Directory authentication server with the same user1. For the www.juniper.net bookmark to be transferred from SA1/ACE/user1 to SA2/AD/user1 you would assign the logical name “Logical1” to both the ACE server on SA1 and the Active Directory server on SA2.

As long as the logical name is the same, the authentication servers can be different types and can have different server names and still be associated with a common user. The username must be the same for user record data to be synchronized across the servers. The logical authentication server (LAS) and username combination is what uniquely identifies a user record.

The following user records are synchronized between the client and server:

- Bookmarks
 - Web
 - File
 - Terminal Services
 - JSAM
- Preferences
- Persistent cookies

This chapter includes the following topics:

- [Enabling User Record Synchronization \(NSM Procedure\) on page 278](#)
- [Configuring the Authentication Server \(NSM Procedure\) on page 278](#)

- [Configuring the User Record Synchronization Server \(NSM Procedure\) on page 279](#)
- [Configuring the Client \(NSM Procedure\) on page 280](#)
- [Configuring the Database \(NSM Procedure\) on page 281](#)

Enabling User Record Synchronization (NSM Procedure)

The first step in enabling user record synchronization is to define the node name and the shared secret used for client/server authentication. The node name is used when associating a client with a server and is different from the logical name assigned to a server. This node name is also not the same as the cluster node name. The shared secret is the password used to authenticate the client with its servers and the primary server with its peer servers. Use the same shared secret for all clients and servers participating in user record synchronization.

To enable user record synchronization:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to enable user record synchronization.
2. Click the **Configuration** tab, and select **System > Configuration > User Record Synchronization > General**.
3. Select the **User Record Synchronization Enabled** check box.
4. Enter a unique node name in the Node Name box.
5. Enter the shared secret in the Shared Secret box.
6. Select whether this node is client only or if this node acts as both a client and server in the Node Function drop-down list.
7. Click **OK** to save the changes.



NOTE: If you need to make any changes in this window at a later time, you must clear the **User Record Synchronization Enabled** check box and click **OK**. Modify your entries, select the **User Record Synchronization Enabled** check box and save your changes. Once you enter a name and shared secret, you cannot clear these fields.

Related Documentation

- [Configuring the Authentication Server \(NSM Procedure\) on page 278](#)
- [Configuring the User Record Synchronization Server \(NSM Procedure\) on page 279](#)

Configuring the Authentication Server (NSM Procedure)

To set up the authentication server, you must define its logical name:

To set up the authentication server:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure an authentication server.
2. Click the **Configuration** tab, and select **Authentication > Auth Servers**.
3. Click the name of the authentication server you want to assign an LAS name.

By assigning the authentication server a logical authentication server (LAS) name, all users that authenticate using the authentication server are associated with this LAS. In this instance, we are referring to the client nodes, not the user record synchronization server nodes.

4. Select the **User Record Synchronization** check box.
5. Enter a logical name to identify this server in the Logical Auth Server Name box.

This allows you to share user record data across authentication servers on different Secure Access gateways. By assigning an LAS name to an authentication server, you are implicitly assigning it to all users that authenticate with that authentication server. The combination of the user login name and its LAS name uniquely identifies the user record of the user across all user record synchronization servers.

6. Click **OK** to save the changes.

**Related
Documentation**

- [Enabling User Record Synchronization \(NSM Procedure\) on page 278](#)
- [Configuring the User Record Synchronization Server \(NSM Procedure\) on page 279](#)

Configuring the User Record Synchronization Server (NSM Procedure)

To set up the user record synchronization server you must define its peer nodes (optional) and the clients that can access this server.

To configure user record synchronization server:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure a user record synchronization server.
2. Click the **Configuration** tab, and select **System > Configuration > User Record Synchronization > This Server**.
3. Under Peer Servers tab, click **New**.
4. Enter the peer server node name in the Server Node Name.
5. Enter the peer IP address in the Internal Address box.
6. Click **OK**. Data is replicated from the primary or backup server to its peer servers. If the primary is not available, user data is sent to the backup. User data is then replicated to the peer servers.

7. For each client you want to synchronize with this server, enter the client's name and IP address and click **OK**. Once added, peer servers will have a colored icon next to their name indicating their connection status. Node status is provided to client nodes and LAS mapping servers as described in [Table 82 on page 280](#).
8. Click **OK** to save the changes.

Table 82: Server Color Codes

Color	Description
Green	Connected
Yellow	Connecting
Gray	Not Connected

- Related Documentation**
- [Configuring the Authentication Server \(NSM Procedure\) on page 278](#)
 - [Configuring the Client \(NSM Procedure\) on page 280](#)

Configuring the Client (NSM Procedure)

To set up the client, you select the primary and backup server you want this client to synchronize with.

To configure the client:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure the client.
2. Click the **Configuration** tab, and select **System > Configuration > User Record Synchronization > This Client**.
3. Click **New**. The New LAS to Server mapping page appears.
4. Select the LAS name you want to synchronize from the Logical Authentication Server Name (or 'Any LAS') list.
5. Enter the primary IP address of the user record server that will synchronize the user records in the Primary Server box. If you prefer to synchronize with any available server, select **Logical Authentication Server Name (or 'Any LAS')**.
6. Enter a backup server IP address in the **Backup Server**. Click **OK**.

Even if you select **Logical Authentication Server Name (or 'Any LAS')**, you must enter a primary server IP address. Once added, the primary and backup servers have a colored icon next to their name indicating their connection status.

7. Click **OK** to save the changes.

- Related Documentation**
- [Configuring the User Record Synchronization Server \(NSM Procedure\) on page 279](#)

- [Configuring the Database \(NSM Procedure\) on page 281](#)

Configuring the Database (NSM Procedure)

In the Database, you can delete inactive records from the client cache, retrieve statistics about the database, export and import the data, and remove user data from the server's database.

To configure the database:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure the database.
2. Click the **Configuration** tab, and select **System > Configuration > User Record Synchronization > Database**.
3. Modify settings as described in [Table 83 on page 281](#).
4. Click **OK** to save the changes.

Table 83: Configuring the Database

Options	Your Action
Auto-delete inactive synchronized user records from the Cache	<p>When you select this option, it removes inactive user records from the cache. The device performs a check every 15 minutes and deletes user records that meet all of the following criteria:</p> <ul style="list-style-type: none">• There are no active user sessions associated with the user record.• The user record does not have any custom settings or the latest version of the user record has been synchronized with the user record database.• The authentication server associated with the user record database does not have type "local." <p>NOTE: This option does not remove user records from the user record database.</p>
Time a user record can be idle before being auto-deleted (days)	<p>When you select this option, it permanently removes user records from the database located on the server. Enter the number of days user records must be idle before being auto-deleted. The default value is none.</p>

- Related Documentation
- [Configuring the User Record Synchronization Server \(NSM Procedure\) on page 279](#)
 - [Configuring the Client \(NSM Procedure\) on page 280](#)

CHAPTER 20

Configuring IF-MAP Federation Settings

This chapter describes the interoperation between heterogeneous network appliances in a federated network. In a federated network, users providing valid credentials can access resources protected by any number of Juniper Networks security devices without re-authenticating through a different device. Juniper Networks IDP Series Intrusion Detection and Prevention Appliance can be incorporated into a federated network to protect against attacks within the network.

This chapter includes the following topics:

- [Configuring IF-MAP Servers \(NSM Procedure\) on page 283](#)
- [Configuring IF-MAP Client Settings on the Secure Access Device \(NSM Procedure\) on page 284](#)
- [Configuring IF-MAP Session Export Policy on the Secure Access Device \(NSM Procedure\) on page 285](#)
- [Configuring IF-MAP Session Import Policy on the Secure Access Device \(NSM Procedure\) on page 288](#)
- [Configuring IF-MAP Server Replicas \(NSM Procedure\) on page 290](#)

Configuring IF-MAP Servers (NSM Procedure)

You must add all IF-MAP clients to the Secure Access IF-MAP server to permit the server to communicate with its clients. To add clients, you must specify the IP address and the security mechanism and credentials for each client.

An IF-MAP server certificate must also be installed on the IF-MAP server. The client verifies the server certificate when it connects to the server. The server certificate must be signed by a certificate authority (CA), the client must be configured to trust certificates signed by that CA, and the hostname in the server certificate must match the hostname in the IF-MAP URL on the client.

To configure IF-MAP server settings on the Secure Access device that will be the IF-MAP server:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Configuration** tab. In the configuration tree, select **System > IF-MAP Federation > Overview**.
2. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure IF-MAP server settings.
3. From the IF-MAP Configuration list, select **IF-MAP Server**.
4. Click the **OK** button to save the changes.
5. From the This Server tab, select **Clients and Replicas** and click the **New** button.
6. Enter a name and an optional description for this client.
7. From the Type list, select **Client**.
8. Type one or more IP addresses of the client. If the client is multihomed, for best results list all of its physical network interfaces. If the client is an Infranet Controller or Secure Access cluster, list the internal and external network interfaces of all nodes. It is necessary to enter all of the IP addresses for all of the interfaces because equipment failures may cause traffic between the IF-MAP client and the IF-MAP server to be rerouted through a different network interface. Listing all of the IP addresses maximizes the probability that IF-MAP Federation still works in the event of a failure.
9. Under Authentication Type, select the Client Authentication Method: **Basic** or **Certificate**.
 - If you select **Basic**, enter a username and password. The same information should be added to the IF-MAP server.
 - If you select **Certificate**, choose which CA to use to verify the certificate for this client. Optionally, specify certificate attributes or restrictions to require values for certain client certificate attributes.
10. Click **OK** to save the IF-MAP client instance on the IF-MAP server.

**Related
Documentation**

- [Configuring IF-MAP Client Settings on the Secure Access Device \(NSM Procedure\) on page 284](#)
- [Configuring IF-MAP Session Export Policy on the Secure Access Device \(NSM Procedure\) on page 285](#)

Configuring IF-MAP Client Settings on the Secure Access Device (NSM Procedure)

You must identify the IF-MAP server to each Infranet Controller and SA appliance IF-MAP client. To add the server, you specify the IF-MAP URL of the server and how to authenticate to the server. Match the URL and security settings to equal those on the IF-MAP server(s) to which the IF-MAP client will connect.

To configure IF-MAP client settings on the Infranet Controllers or SA appliances that will be IF-MAP clients:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure IF-MAP client settings.
2. Click the **Configuration** tab. In the configuration tree, select **System > IF-MAP Federation > Overview**.
3. From the IF-MAP Configuration list, select **IF-MAP Client**.

4. Type the server URL for the IF-MAP Web service on the IF-MAP server. For a Juniper IF-MAP server, use:

`https://<FQDN>/dana-ws/soap/ifmap`

FQDN is the fully qualified domain name of the replica's internal or external interface; for a cluster, the FQDN of the internal or external VIP should be used.

5. Under Authentication Type, select the Client Authentication Method: **Basic** or **Certificate**.
 - If you select **Basic**, enter a username and password. The same information should be added to the IF-MAP server.
 - If you select **Certificate**, choose which Certificate Authority (CA) to use to verify the certificate for this client. Optionally, specify certificate attributes or restrictions to require values for certain client certificate attributes.
 - Ensure that the certificate of the CA that signed the IF-MAP server certificate is added from the System > Configuration > Certificates > Trusted Server CAs page.

The IF-MAP client validates the IF-MAP server certificate: if validation fails, the connection fails. Ensure that the hostname in the IF-MAP URL on the client machine matches the hostname of the server certificate on the IF-MAP server, and that the CA that signed the server certificate is configured as a trusted server CA on the IF-MAP client.

6. Click **OK** to save the changes.

Related Documentation

- [Configuring IF-MAP Session Export Policy on the Secure Access Device \(NSM Procedure\) on page 285](#)
- [Configuring IF-MAP Servers \(NSM Procedure\) on page 283](#)

Configuring IF-MAP Session Export Policy on the Secure Access Device (NSM Procedure)

Session-export policies determine how users are identified on the IF-MAP server when their session is published through IF-MAP. The session-export policy sets the IF-MAP identity.

To configure a session-export policy:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure a session-export policy.
2. Click the **Configuration** tab. In the configuration tree, select **System > IF-MAP Federation > Session-Export Policies**.
3. Add or modify settings as specified in [Table 84 on page 286](#).
4. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

You must create corresponding session-import policies that allow IF-MAP client Infranet Controllers that are connected to an Infranet Enforcer in front of protected resources to collect IF-MAP data from the IF-MAP server.

Table 84: IF-MAP Session-Export Policy Configuration Details

Option	Function	Your Action
Name	Specifies a unique name for the policy.	Enter a name for the policy.
Description	Describes the policy.	Enter a brief description for the policy.
Administrative Domain	Identifies the IP address, username, or MAC address data. In a large network environment with several domains, a username, an IP address, or a MAC address could be duplicated. By entering the domain, you ensure that the correct user is identified.	Type the administrative domain for the session export policy. If you want different aspects of a user session to be exported with different administrative domains, you then create several export rules.
Roles	Determines the roles for which this policy should apply.	Select roles from the Non-members area and add the roles to the Members area.
Stop on match	Stops matching the roles when an IF-MAP client has successfully matched the roles selected for this policy to roles based on session-import policies configured on the target device.	Select this option to stop matching roles after a successful match is found.

Identity tab

Table 84: IF-MAP Session-Export Policy Configuration Details (*continued*)

Option	Function	Your Action
Set IF-MAP Identity	Specifies the applicable identity.	<p>Select this action and the identity options appear.</p> <ul style="list-style-type: none"> • Identity—Enter the identity name. Identity is normally specified as <Name>, which assigns the user's login name. Any combination of literal text and context variables may be specified. • Identity Type—Select the identity type. If you choose Other for Identity Type, enter a unique identity type in the text box.
Roles tab		
Set IF-MAP Roles	Specifies the applicable roles.	<p>Select this action and the following role options appear.</p> <ul style="list-style-type: none"> • Copy matching roles—Select this option to copy all of the user roles that match the roles specified in the Roles section of this policy into the IF-MAP roles data. • Copy ALL roles—Select this option to copy all of the roles from the user session to the IF-MAP capabilities data. • Set roles specified below—Select this option to set the specified roles. The Roles option appears. From Roles, click New and enter a specified role.
Capabilities tab		
Set IF-MAP Capabilities	Specifies the applicable roles.	<p>Select this action and the following role options appear:</p> <ul style="list-style-type: none"> • Copy matching roles—Select this option to copy all of the user roles that match the roles specified in the Roles section of this policy into the IF-MAP capabilities data. • Copy ALL roles—Select this option to copy all of the roles from the user session to the IF-MAP roles data. • Set capabilities specified below—Select this option to set the specified capabilities. The Capabilities option appears. From Capabilities, click New and enter a specified capability.
Device Attributes tab		

Table 84: IF–MAP Session-Export Policy Configuration Details (*continued*)

Option	Function	Your Action
Set IF-MAP Device Attributes	Specifies a passed Host Checker policy on the Infranet Controller or SA appliance.	<p>Select this action and the following options appear.</p> <ul style="list-style-type: none"> • Copy Host Checker policy names—Select this option to copy the name of each Host Checker policy that passed for the session to a device attribute. • Set device attributes specified below—Select this option to set the specified device attributes. The Device Attributes option appears. From Device Attributes, click New and enter a specified device attribute.

Related Documentation

- [Configuring IF-MAP Client Settings on the Secure Access Device \(NSM Procedure\) on page 284](#)
- [Configuring IF-MAP Session Import Policy on the Secure Access Device \(NSM Procedure\) on page 288](#)

Configuring IF-MAP Session Import Policy on the Secure Access Device (NSM Procedure)

The session-export policies that you create allow IF-MAP data that represents a session to be stored on the IF-MAP server. Session-import policies specify how the Secure Access device derives a set of roles and a username from the IF-MAP data in the IF-MAP server. Session-import policies establish rules for importing user sessions from a different Infranet Controller or SA appliance. Import policies allow you to match authenticated users with corresponding roles on the target device. For example, you might configure an import policy to specify that when IF-MAP data for a session includes the “Contractor” capability, the imported session should have the “limited” role. Session-import policies allow the device to properly assign roles based on information that the IF-MAP server provides.

To configure a session-import policy:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure a session-import policy.
2. Click the **Configuration** tab. In the configuration tree, select **System > IF–MAP Federation > Session-Import Policies**.
3. Add or modify settings as specified in [Table 85 on page 289](#).
4. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 85: IF-MAP Session-Import Policy Configuration Details

Option	Function	Your Action
Name	Specifies a unique name for the session-import policy.	Enter a name for the session-import policy.
Description	Describes the policy.	Enter a brief description for the policy.
Stop on match	Stops matching the roles when an IF-MAP client has successfully matched the roles.	Select this option to stop matching roles after a successful match is found.
Match Criteria > Identity tab		
Match IF-MAP Identity	Specifies that identity should be used as the criteria for assigning roles.	<p>Select this action and the following identity options appear.</p> <ul style="list-style-type: none"> • Identity—Enter the identity name. For example, for a regular employee named Bob Smith you might enter the Identity as username bsmith and select username for the identity type. • Identity Type—Select the identity type. If you choose Other for identity type, enter a unique identity type in the text box. • Administrative Domain—Type the administrative domain for the session-import policy. <p>All aspects of the IF-MAP identity (name, type, and administrative domain) must exactly match the session-import policy.</p>
Match Criteria > Roles tab		
Match IF-MAP Roles	Specifies that role match should be used as the criteria for assigning roles.	<p>Select this action and the following role option appears.</p> <ul style="list-style-type: none"> • Roles— From Roles, click New and enter a specified role.
Match Criteria > Capabilities tab		
Match IF-MAP Capabilities	Specifies that capability match should be used as the criteria for assigning roles.	<p>Select this action and the following option appears.</p> <ul style="list-style-type: none"> • Capabilities—From Capabilities, click New and enter a specified capability.
Match Criteria > Device Attributes tab		
Match IF-MAP Device Attributes	Specifies that device attribute match should be used as the criteria for assigning roles.	<p>Select this action and the following option appears.</p> <ul style="list-style-type: none"> • Device Attributes—From Device Attributes, click New and enter a specified device attribute.
Actions > Assign Roles tab		
Use these roles	Assigns roles from the available list.	Select Secure Access devices roles from the Non-members area and move it to the Members area.

Table 85: IF–MAP Session-Import Policy Configuration Details (*continued*)

Option	Function	Your Action
Actions > Copy IF-MAP Roles tab		
Copy IF-MAP Roles	Copies the specified roles.	Select Copy IF-MAP roles and select All roles , Specified roles , or All roles other than those specified below , and then list the IF-MAP roles.
Actions > Copy IF-MAP Capabilities tab		
Copy IF-MAP Capabilities	Copies the IF-MAP capabilities.	Select Copy IF-MAP capabilities and select All capabilities , Specified capabilities or All capabilities other than those specified below , and then list the IF-MAP capabilities.

- Related Documentation**
- [Configuring IF-MAP Session Export Policy on the Secure Access Device \(NSM Procedure\) on page 285](#)
 - [Configuring IF-MAP Server Replicas \(NSM Procedure\) on page 290](#)

Configuring IF-MAP Server Replicas (NSM Procedure)

You can configure an IF-MAP server to replicate all of its IF-MAP data to other IF-MAP servers. For example, if you have a network in Boston and a network in London, you can run IF-MAP servers in both places and configure the IF-MAP servers in both locations to replicate data to one another. These connected IF-MAP servers are known as replicas.

To configure IF-MAP server replicas to communicate with each other:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure IF-MAP server replicas.
2. Click the **Configuration** tab. In the configuration tree, select **System > IF–MAP Federation > This Server**.
3. Add or modify settings as specified in [Table 86 on page 290](#).
4. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 86: Replica IF–MAP Server Configuration Details

Option	Function	Your Action
Name	Specifies a unique name for the replica IF-MAP server.	Enter a name for the replica IF-MAP server.
Description	Describes the replica or replica network.	Enter a brief description for the replica or replica network.

Table 86: Replica IF-MAP Server Configuration Details (*continued*)

Option	Function	Your Action
Type	Specifies whether the configuration is for an IF-MAP client or for a replica IF-MAP server.	From the Type list, select Replica .
Hostname	Specifies the hostname that exactly matches the replica's device certificate.	Enter the hostname of the replica's device certificate. The hostname is used when this IF-MAP server initiates a connection to the replica. The fully qualified domain name (FQDN) of the replica's internal or external interface should be used; for a cluster, the FQDN of the internal or external VIP should be used.
IP Address(es)	Specifies the IP addresses from which the replica may initiate connections to this server.	Enter one or more IP addresses from which the replica may initiate connections to this server. If the replica is standalone, for survivability list both the internal and external network interfaces. If the replica is a cluster, for survivability list the internal and external network interfaces of both cluster nodes.
Authentication Type	Specifies the authentication type.	Select the authentication method: <ul style="list-style-type: none"> • Basic—If you select Basic, enter a username and password. • Certificate—If you select Certificate, select the certificate authority that issued the IF-MAP replica's certificate. Enter any restrictions, one per line. If any restrictions match, for example CN=ic.example.com, the certificate is accepted.

Related Documentation

- [Configuring IF-MAP Session Import Policy on the Secure Access Device \(NSM Procedure\) on page 288](#)
- [Configuring IF-MAP Servers \(NSM Procedure\) on page 283](#)

PART 4

Managing Secure Access Devices

- [Managing Secure Access Devices on page 295](#)
- [Troubleshooting Secure Access Device Federated Networks on page 301](#)

Managing Secure Access Devices

- [Managing Large Binary Data Files \(NSM Procedure\) on page 295](#)
- [Removing a Secure Access Device from NSM Management \(NSM Procedure\) on page 296](#)
- [Archiving Secure Meetings \(NSM Procedure\) on page 297](#)
- [Managing Secure Access Node from a Cluster on page 298](#)

Managing Large Binary Data Files (NSM Procedure)

Large binary data files that form a part of the configuration of Secure Access and Infranet Controller devices are handled differently from the remainder of the configuration in NSM. The size of some of these binary files could make configurations large enough to overload resources on the NSM server. Consequently, only the large binary files you specify are imported into NSM, and those files are configured as shared objects, which avoids duplication if they are applied to multiple devices.

To download a large binary data file and link that file into the Secure Access or Infranet Controller device configuration tree:

1. In the Device Manager, right-click the device icon and select **Import Device** from the list to import the Secure Access or Infranet Controller device configuration. When the import job is finished, the device object configuration contains the MD5 stubs for each of the large binary data files.
2. Upload each mandatory large binary data file onto the NSM client workstation. Use the device Web UI to upload binary files from the Secure Access or Infranet Controller device. Other files, such as ESAP configuration files, should be downloaded from the site of origin.
3. Create a shared object in the NSM Object Manager for the binary file as follows:
 - a. In the Configure panel of the NSM navigation tree, select **Object Manager > Binary data**, and then click the Add icon.
 - b. In the New Binary Data dialog box, enter a name for the object, select a color for the object icon, add a comment if desired, and select the file you uploaded in Step 2.

- c. Click **OK**.
4. Link the shared object to the corresponding node in the device configuration tree as follows:
 - a. In the Device Manager, double-click the Secure Access or Infranet Controller device to open the device editor, and then select the **Configuration** tab.
 - b. Navigate to the node in the configuration where you want to load the binary file. For example, to load an ESAP package, click **Authentication** and then select **Endpoint Security**. In the Host Checker tab, select **Endpoint Security Assessment Plug-Ins**, and then click the **Add** icon.
 - c. Select the shared object. To continue the ESAP example, in the New Endpoint Security Assessment Plug-Ins dialog box, enter a version number, and select a shared binary data object from the Path to Package list.
 - d. Click **OK**. If the object you want is not in the list, you can add it to the shared binary data list by clicking the **Add** icon. The Binary Data dialog box appears as in Step 3.
 - e. Click **OK** to save the newly configured links.

Related Documentation

- [Removing a Secure Access Device from NSM Management \(NSM Procedure\) on page 296](#)
- [Archiving Secure Meetings \(NSM Procedure\) on page 297](#)
- [Configuring Secure Access Sign-In Pages \(NSM Procedure\) on page 211](#)
- [Configuring Host Checker Third-Party Applications Using Predefined Rules \(NSM Procedure\) on page 234](#)

Removing a Secure Access Device from NSM Management (NSM Procedure)

Deleting a device removes all device configuration information from the management system, but might be the best solution if you need to perform extensive troubleshooting or reconfigure the device locally.

To remove a Secure Access device from NSM Management:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab.
3. From the device tree, select the Secure Access device that you would like to remove from NSM Management.
4. Right-click and select **Delete**, or click the **Delete** button. The Delete dialog box appears. If the device is referenced in a firewall rule, this dialog box displays the rules that reference it. You can click the links that appear to display the Security Policies, and to view or edit those references.

5. Click **Next** to remove the device. The Delete dialog box displays the progress of the deletion.
6. When Network and Security Manager finishes, click **Finish** to close the dialog box.

Related Documentation

- [Archiving Secure Meetings \(NSM Procedure\) on page 297](#)
- [Configuring User Access, Admin Access, Events and Sensors \(NSM Procedure\) on page 305](#)

Archiving Secure Meetings (NSM Procedure)

The Secure Access device enables you to archive Secure Meeting instances. You can:

- Set up a recurring archival process.
- Perform a one-time archive.
- Archive the deleted meetings into an XML file for later download or deletion. One file is created for each archive run.
- Define the number of days a SecureMeeting instance remains on the device before archiving (instances older than x number of days are archived).
- Define which node in a cluster performs the archive.

To archive secure meetings:

1. In the navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to archive secure meetings.
2. Click the **Configuration** tab. Select **System > Maintenance > Archiving > Secure Meetings**.
3. Add or modify settings as specified in [Table 87 on page 297](#).
4. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 87: Archiving Secure Meetings Details

Option	Function	Your Action
Perform automatic cleanup	Schedules a recurring archival process and specifies how often the archiving process should run.	Select the Perform automatic cleanup option to enable this feature.
Frequency of automatic cleanup	Specifies how often the archiving process should run.	Select either Month or Week .
Delete meetings older than this number of days (days)	Specifies the status of the old meetings before they are being archived.	Enter the number of days.

Table 87: Archiving Secure Meetings Details (*continued*)

Option	Function	Your Action
Archive meeting records before deleting	Archives secure meetings in a cluster configuration.	Select the Archive meeting records before deleting option to enable this feature.
Archive meeting records on node	Specifies the node that performs the archive.	Enter the node.

Related Documentation

- [Configuring User Access, Admin Access, Events and Sensors \(NSM Procedure\) on page 305](#)
- [Managing Large Binary Data Files \(NSM Procedure\) on page 295](#)

Managing Secure Access Node from a Cluster

Table 88 on page 298 describes the information displayed on the Status tab and the various management tasks you can perform including disabling, enabling, and removing a Secure Access device node from a cluster.

Table 88: Cluster Status Page Information

User Interface Element	Description
Status Information	Displays the cluster name, type, configuration, internal VIP, and external VIP for an active/passive cluster.
Add Members	Specifies a device to add the cluster. You must perform this step for device systems you intend to add to the cluster. By clicking this button, you can add multiple nodes at the same time.
Enable	Adds a node that was previously disabled. When you add a node, all stated information is synchronized on the node.
Disable	Disables a node within the cluster. The node retains awareness of the cluster, but does not participate in state synchronizations or receive user requests unless members sign in to the node directly.
Remove	Removes the selected node or nodes from the cluster. Once removed, the node runs in standalone mode.
Fail-Over VIP	Fails over the VIP to the other node in the active/passive cluster. This option is enabled only if cluster is configured as Active/passive.
Member Name	Lists all nodes belonging to the cluster. You can click a node to modify its name and network settings.
Internal Address	Shows the internal IP address of the cluster member using Classless Interdomain Routing (CIDR) notation.

Table 88: Cluster Status Page Information (*continued*)

User Interface Element	Description
External Address	Shows the external IP address of the cluster member using CIDR notation. Note that this column only shows the external IP address of the cluster leader unless you specify a different address for the node on its individual network settings page, which is accessible by clicking its name in the Member Name column. If you change the external IP address on the Network > Network Settings page, the change affects all cluster nodes.
Status	<p>Shows the current state of the node:</p> <ul style="list-style-type: none"> • Green light/enabled—The node is handling user requests and participating in cluster synchronization. • Yellow light/transitioning—The node is joining cluster or a FIPS node has joined a cluster but the cluster's key store remains to be imported onto the node's HSM. • Red light/disabled—The node is not handling user requests or participating in cluster synchronization. • Red light/enabled, unreachable—The node is enabled, but due to a network issue, it cannot be reached. <p>The current state of the node (light color) does not reflect failures in the external interface connectivity. Such failures are logged as events.</p> <p>NOTE: A node's state is considered "standalone" when it is deployed outside of a cluster or after being removed from a cluster.</p>
Notes	<p>Shows the status of the node's connection to the cluster:</p> <ul style="list-style-type: none"> • OK—The node is actively participating in the cluster. • Transitioning—The node is switching from the standalone state to the enabled state. • Unreachable—The node is not aware of the cluster. A cluster member may be "unreachable" even when it is online and can be pinged. Possible reasons include: <ul style="list-style-type: none"> • Password is incorrect. • It does not know about all cluster nodes. • It is configured with a different group communication mode. • It is running a different service package version. • The machine is turned off.
Sync Rank	<p>Specifies the synchronization order for nodes when rejoining a cluster. Accepts sync ranks from 0 (lowest rank) to 255 (highest rank). The highest rank takes precedence. Where two nodes have identical sync ranks, the alpha-numeric rank of the member name is used to determine precedence.</p> <p>NOTE: This option is available only with a Central Manager license.</p>
Update	Updates the sync rank after you change the precedence of the nodes in the Sync Rank column.

Related Documentation

- [Adding a Secure Access Cluster Overview on page 23](#)
- [Managing Large Binary Data Files \(NSM Procedure\) on page 295](#)

CHAPTER 22

Troubleshooting Secure Access Device Federated Networks

- [Troubleshooting the IF-MAP Federation Network \(NSM Procedure\) on page 301](#)

Troubleshooting the IF-MAP Federation Network (NSM Procedure)

Diagnostic tools on the SA Series appliances can assist you with troubleshooting a federated network.

IF-MAP Client User Messages—On the IF-MAP client, logs the information that is published and removed from the IF-MAP server.

- Enable IF-MAP Client User Messages from **Log/Monitoring > User Access > Settings** on the SA Series appliances IF-MAP client.

IF-MAP Server Trace—On the IF-MAP server, logs the XML for all IF-MAP requests and responses.

- Enable the IF-MAP Server Trace from **Log/Monitoring > Events > Settings** on the IF-MAP server.

IF-MAP Server Trace should only be enabled for troubleshooting purposes, as running this diagnostic incurs a large performance impact.

Related Documentation

- [Configuring IF-MAP Servers \(NSM Procedure\) on page 283](#)
- [Configuring IF-MAP Client Settings on the Secure Access Device \(NSM Procedure\) on page 284](#)

PART 5

Monitoring Secure Access Devices

- [Configuring Logs in Secure Access Devices on page 305](#)
- [Viewing Logs in Secure Access Devices on page 313](#)

Configuring Logs in Secure Access Devices

- [Configuring User Access, Admin Access, Events and Sensors \(NSM Procedure\) on page 305](#)
- [Configuring Custom Filters and Formats for Log Files \(NSM Procedure\) on page 308](#)
- [Configuring Client-Side Logs \(NSM Procedure\) on page 310](#)
- [Configuring Custom Log Filters \(NSM Procedure\) on page 311](#)

Configuring User Access, Admin Access, Events and Sensors (NSM Procedure)

To configure user access, admin access, sensors, and events:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure user access, admin access, sensors, and events.
2. Click the **Configuration** tab, and select **System > Log/Monitoring**. The corresponding workspace appears.
3. Add or modify settings as specified in [Table 89 on page 305](#) to configure user access, admin access, sensors, and events.
4. Configure syslog servers where you want to store your log files as specified in [Table 90 on page 308](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modification.

Table 89: Configuring User Access, Admin Access, Sensors, and Events Details

Option	Function	Your Action
Events > Settings tab		
Max Log Size (MB)	Specifies the maximum file size for the local log file. NOTE: The system log displays data up to the amount specified. (The limit is 200 MB).	Specify the file size.

Table 89: Configuring User Access, Admin Access, Sensors, and Events Details (*continued*)

Option	Function	Your Action
Connection Requests	Captures the requests required for connection to the security device.	Select Connection Requests to enable this feature
System Status	Captures the system status.	Select System Status to enable this feature
Rewrite	Captures the rewriting policies.	Select Rewrite to enable this feature
System Errors	Captures all the system errors that occurs.	Select System Errors to enable this feature
Email Proxy Events	Captures all the events specific to e-mail proxies.	Select Email Proxy Events to enable this feature
Statistics	Captures the statistics of the event.	Select Statistics to enable this feature
Performance	Captures the event performance.	Select Performance to enable this feature
Reverse Proxy	Captures the reverse proxy information of the event.	Select Reverse Proxy to enable this feature
Meeting Events	Captures the meeting information of events.	Select Meeting Events to enable this feature
User Access > Settings tab		
Max Log Size (MB)	Specifies the maximum file size for the local log file. NOTE: The system log displays data up to the amount specified. (The limit is 500 MB).	Specify the file size.
Login/Logout	Captures user login/logout events in the local log file.	Select Login/Logout to enable this feature.
SAM/Java	Captures information about user access to SAM/Java in the local log file.	Select SAM/Java to enable this feature.
User Settings	Captures user's settings in the local log file.	Select User Settings to enable this feature.
Secure Terminal	Captures information about user access to secure terminals in the local file.	Select Secure Terminal to enable this feature.
Network Connect	Captures information about user access to Network Connect in the local log file.	Select Network Connect to enable this feature.

Table 89: Configuring User Access, Admin Access, Sensors, and Events Details (*continued*)

Option	Function	Your Action
SAML	Captures information about user access to SAML in the local log file.	Select SAML check box to enable this feature.
Web Requests	Captures information about user access to the Web in the local log file.	Select Web Requests to enable this feature.
File Requests	Captures information about user access to files in the local log file.	Select File Requests to enable this feature.
Meeting	Captures information about user access to meetings in the local log file.	Select Meeting to enable this feature.
Email Requests	Captures information about user access to e-mails in the local log file.	Select Email Requests to enable this feature.
IF-MAP Client User Messages	Captures information about IF-MAP session federated out or exported to federation server including username, IP address, capabilities, roles, and device attributes in the local log file.	Select IF-MAP Client User Messages to enable this feature.
Admin Access > Settings tab		
Max Log Size (MB)	Specifies the maximum file size for the local log file. (The limit is 500 MB.) NOTE: The system log displays data up to the amount specified.	Enter the file size.
Administrator Changes	Captures changes, including administrator changes to user, system, and network settings, such as changes to session timeouts, the option to enable/disable URL browsing and user-created bookmarks, and machine and server information in the local log file.	Select the Administrator Changes check box to enable this feature.
Administrator Logins	Captures information whenever an administrator signs in, signs out, or changes licenses on the device in the local log file.	Select the Administrator Logins check box to enable this feature.
License Changes	Changes licenses on the appliance in the local log file.	Select the License Changes check box to enable this feature.
Sensors > Settings tab		
Max Log Size (MB)	Specifies the maximum file size for the local log file. (The limit is 500 MB.) NOTE: The system log displays data up to the amount specified.	Enter the file size.

Table 90: Configuring Syslog Servers Details

Option	Function	Your Action
User Access / Admin Access / Sensors > Syslog Servers > Settings tab		
Server name/IP	Specifies the syslog server where you want to store your log files (optional).	Enter the name or IP address of the syslog server.
Facility	Specifies the facility to map facilities on your syslog server. NOTE: The Secure Access device provides eight facilities (LOCAL0- LOCAL7).	Select the facility from the drop-down list.
Filter	Specifies the filter you want to apply to the log file.	Select the filter.

Related Documentation

- [Configuring Custom Filters and Formats for Log Files \(NSM Procedure\) on page 308](#)
- [Configuring Client-Side Logs \(NSM Procedure\) on page 310](#)

Configuring Custom Filters and Formats for Log Files (NSM Procedure)

To configure custom filters and formats for log files:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure custom filters and formats for log files.
2. Click the **Configuration** tab, and select **System > Log/Monitoring > Filters**. The corresponding workspace appears.
3. Add or modify settings as specified in [Table 91 on page 308](#).
4. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modification.

Table 91: Custom Filters and Formats for Log Files Configuration Details

Option	Function	Your Action
Filter Name	Specifies the name of the filter.	Enter the name.
Start Date	Specifies the start date in which the Secure Access device writes logs in the log file.	Enter the start date.
End Date	Specifies the end date in which the Secure Access device writes logs in the log file.	Enter the end date.

Table 91: Custom Filters and Formats for Log Files Configuration Details (*continued*)

Option	Function	Your Action
Query	Allows the user to view the logs in different formats.	<p>Enter the custom expression.</p> <p>NOTE: Any string (including a * wildcard character) you manually enter in a query must be enclosed in double-quotes.</p>
Format Type	Specifies the format of the data in the log.	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • Standard—This log filter format logs the date, time, node, source IP address, user, realm, and the Secure Access device event ID and message. • WELF—This customized WebTrends Enhanced Log Format (WELF) filter combines the standard WELF format with information about the Secure Access device realms, roles, and messages. • W3C—The World Wide Web Consortium's extended log file format is a customizable ASCII format with a variety of different fields. Visit http://www.w3.org for more information about this format. Only the User Access log offers this filter as an option. • Custom—Allows you to enter the format you want to use.
Custom Format	<p>Customizes the format of the data in the log.</p> <p>NOTE: This box is enabled only when you select Custom from the Format Type drop-down list.</p>	<p>Enter the format.</p> <p>NOTE: When entering a format, surround variables with percentage symbols (for example %user%). All other characters are treated as literals.</p>

- Related Documentation**
- [Configuring Client-Side Logs \(NSM Procedure\) on page 310](#)
 - [Viewing Device Status on page 313](#)

Configuring Client-Side Logs (NSM Procedure)

Client-side logging is useful when working with the Juniper Networks Support team to debug problems with an Secure Access device client-side feature. When you enable logging for a feature, the Secure Access device writes a log to any client computer that uses the feature. (These settings are global, which means that the Secure Access device writes a log file to all clients that use the enabled feature.) The Secure Access device then appends to the log file each time the feature is invoked during subsequent user sessions. Once the Secure Access device has written a log file to a user's computer, it does not remove it. If users want to remove the log files, they must manually delete them from their computers.

To configure client-side logs:

1. In the navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure a client-side logs.
2. Click the **Configuration** tab. Select **system > Log/Monitoring > Client Logs**.
3. Add or modify settings as specified in [Table 92 on page 310](#).
4. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 92: Configuring Client-Side Logs Details

Option	Function	Your Action
Host Checker	Secure Access device writes client-side logs of Host Checker.	Select the Host Checker to enable this feature.
Cache Cleaner	Secure Access device writes client-side logs of Cache Cleaner.	Select the Cache Cleaner to enable this feature.
Meetings	Secure Access device writes client-side logs of Secure Meeting.	Select the Meetings to enable this feature.
Windows Secure Application Manager	Secure Access device writes client-side logs of SAM.	Select the Windows Secure Application Manager check box to enable this feature.
Java Secure Application Manager and Applet Rewriting	Secure Access device writes client-side logs of Java Secure Application Manager and Applet.	Select the Java Secure Application Manager and Applet Rewriting to enable this feature.
Network Connect	Secure Access device writes client-side logs of Network Connect.	Select the Network Connect to enable this feature.
Terminal Servers	Secure Access device writes client-side logs of Terminal Servers.	Select the Terminal Servers to enable this feature.

Table 92: Configuring Client-Side Logs Details (*continued*)

Option	Function	Your Action
Upload logs disk space (MB)	Specifies the amount of disk space (in Megabytes) you want to allocate for uploaded client log files.	Enter the disk space. NOTE: You can allocate from 0 to 200 MB.
Alert when log uploaded	Secure Access device displays an alert message when an end-user pushes a log file up to the Secure Access device.	Select Alert when log uploaded to enable this feature.

Related Documentation

- [Viewing Device Monitor Alarm Status on page 316](#)
- [Configuring User Access, Admin Access, Events and Sensors \(NSM Procedure\) on page 305](#)

Configuring Custom Log Filters (NSM Procedure)

You can create custom log filters or edit the set of predefined log filters to specify which data is written to your log files as well as its format.

To configure the log filters:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure log filter.
3. Click the **Configuration** tab. In the configuration tree, select **System > Log/Monitoring > Filters**.
4. Add or modify settings as specified in [Table 93 on page 311](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 93: Log Filter Configuration Details

Option	Function	Your Action
Filter Name	Specifies a name for the filter.	Enter a name for the filter.
Start Date	Specifies the date from which logs have to be written.	Enter a start date.
End Date	Specifies the date up to which logs have to be written.	Enter an end date.

Table 93: Log Filter Configuration Details (*continued*)

Option	Function	Your Action
Query	Specifies the custom expression language to control which subset of data the Secure Access device writes to the log.	<p>To use the Secure Access device custom expression language:</p> <ol style="list-style-type: none"> 1. Click the New Expression button. The Custom Expression editor is displayed. 2. Select the variable from the Expression Dictionary and click the Insert Expression button. 3. Click the Validate button to validate the expression. 4. Click OK to save the custom expression.
Format Type	Specifies the format of the data in the log.	<p>Select one of the following format types:</p> <ul style="list-style-type: none"> • Standard: This log filter format logs the date, time, node, source IP address, user, realm, and the Secure Access device event ID and message. • WELF: This customized WebTrends Enhanced Log Format (WELF) filter combines the standard WELF format with information about the Secure Access device's realms, roles, and messages. • W3C: The World Wide Web Consortium's extended log file format is a customizable ASCII format with a variety of different fields. Visit http://www.w3.org for more information about this format. Only the User Access log offers this filter as an option. • Custom: Enter the format you want to use in Custom Format. When entering a format, surround variables with percentage symbols (for example %user%). All other characters in the field are treated as literals.

Related Documentation

- [Configuring Client-Side Logs \(NSM Procedure\) on page 310](#)
- [Configuring Custom Filters and Formats for Log Files \(NSM Procedure\) on page 308](#)

Viewing Logs in Secure Access Devices

- [Viewing Device Status on page 313](#)
- [Viewing Device Monitor Alarm Status on page 316](#)
- [Monitoring the Secure Access as an SNMP Agent \(NSM Procedure\) on page 317](#)

Viewing Device Status

[Table 94 on page 313](#) lists and describes device information that you can view through the Device Monitor.

Table 94: Device Status Information

Column	Description
Name	Unique name assigned to the device in NSM.
Domain	Domain in NSM in which the device is managed.
Platform	Model number of the device.
OS Version	Operating system firmware version running on the device.

Table 94: Device Status Information (*continued*)

Column	Description
Config Status	<p>Current configuration status of the device in NSM:</p> <ul style="list-style-type: none"> • None—No state has been set (does not show in Device Monitor). • Waiting for 1st connect—NSM is waiting for the device to connect. You must enter a command on the device to make it connect to NSM. • Import Needed—You must import the configuration of the device into NSM. When you add a device for the first time, verify that your status indicates "Import Needed" before you attempt to import the device. During migration, this state indicates that import of the security device configuration is still required. • OS Version Adjustment Needed—The firmware version detected running on the device is different than what was previously detected in NSM. This could happen in the event that the automatic adjustment option was cleared during a change device firmware directive or an Update Device directive was issued to an IDP device with a firmware version mismatch. • Platform Mismatch—The device platform selected when adding the DMI device in NSM does not match the device itself. A device in this state cannot connect to NSM. • Device Type Mismatch—The type of device specified when adding the device in NSM does not match the device itself. The device type might indicate whether the device is part of a vsys device, part of a cluster, or part of a virtual chassis. A device in this state cannot connect to NSM. • Detected duplicate serial number—The device has the same sequence number as another managed device. A device in this state cannot connect to NSM. • Managed—The device is currently being managed by NSM. • Managed, In Sync—The physical device configuration is synced with the modeled configuration in NSM.
Config Status (continued)	<ul style="list-style-type: none"> • Managed, Device Changed—The physical device configuration is out of sync with the modeled configuration in NSM. Changes were made to the physical device configuration (the configuration on the physical device is newer than the modeled configuration). • Managed, NSM Changed—The modeled device configuration is out of sync with the physical device configuration. Changes were made to the modeled configuration (the configuration on the NSM is newer than the physical device configuration). • Managed, NSM and Device Changed—Both device configurations (physical and modeled) are out of sync with each other. Changes were made to the physical device configuration and to the modeled configuration. • Managed, Sync Pending—Completion of the Update Device directive is suspended and waiting for the device to reconnect. This state occurs only for ScreenOS devices that have the Update When Device Connects option selected during the device update.

Table 94: Device Status Information (*continued*)

Column	Description
Connection Status	<p>Connection status of the device in NSM:</p> <ul style="list-style-type: none"> Up—Device is currently connected to NSM. Down—Device is not currently connected to NSM but has connected in the past. Never Connected—Device has never connected to NSM. <p>The Device Server checks the connection status of each device every 120 seconds by default. You can change this behavior by editing the value for the <code>devDaemon.deviceHeartbeatTimeout</code> parameter in the Device Server configuration file. Refer to the <i>Network and Security Manager Installation Guide</i> for more information on editing configuration files.</p> <p>NOTE: If the network connection goes down for a period longer than six to eight minutes, the device connection will permanently time out. If this occurs and the device goes down for any reason, the device still appears as Up in the Device Monitor.</p>
Alarm	<p>Displays the current alarm status for each device in NSM:</p> <ul style="list-style-type: none"> If device has any alarms, the most severe alarm severity is displayed (either Major or Minor). None—The device has no alarms. Unknown—The device status is unknown. For example, the device might not be connected. N/A—The device's alarm is not pollable or discoverable, for example, this column shows "N/A" for ScreenOS and IDP devices. Alarm is colored: <ul style="list-style-type: none"> Red for Major. Orange for Minor. Green for Ignore, None, Unknown, or N/A.
H/W Inventory Status	<p>Displays the inventory status for hardware on the device:</p> <ul style="list-style-type: none"> In Sync—The inventory information in the NSM database is synchronized with the information on the device. Out Of Sync—The inventory information in the NSM database is not synchronized with the information on the device. N/A—The connected device is a ScreenOS or IDP device, or the device is not connected and imported.
S/W Inventory Status	<p>Displays the inventory status for software on the device:</p> <ul style="list-style-type: none"> In Sync—The inventory information in the NSM database is synchronized with the software on the device. Out Of Sync—The inventory information in the NSM database is not synchronized with the software on the device. N/A—The connected device is a ScreenOS or IDP device, or the device is not connected and imported.

Table 94: Device Status Information (*continued*)

Column	Description
License Inventory Status	<p>Displays the inventory status for software on the device:</p> <ul style="list-style-type: none"> • In Sync—The inventory information in the NSM database is synchronized with the licenses on the device. • Out Of Sync—The inventory information in the NSM database is not synchronized with the licenses on the device. • N/A—The connected device is a ScreenOS or IDP device, or the device is not connected and imported.
First Connect	The first time the security device connected to the NSM Device Server.
Latest Connect	The last time the security device connected to the NSM Device Server.
Latest Disconnect	The last time the security device disconnected from the NSM Device Server.

- Related Documentation**
- [Viewing Device Monitor Alarm Status on page 316](#)
 - [Monitoring the Secure Access as an SNMP Agent \(NSM Procedure\) on page 317](#)

Viewing Device Monitor Alarm Status

Alarms refresh automatically through periodic polling.

To view the Alarm status and time:

1. From **Device Monitor**, right-click the device row entry and select the **View Alarm** option.
The device **Alarm Status** dialog box displays the alarm list and polling time for the device.
2. To retrieve the current alarm status in the device, click the **Refresh** button.

The poll time is derived from the device server time.

- Related Documentation**
- [Monitoring the Secure Access as an SNMP Agent \(NSM Procedure\) on page 317](#)
 - [Viewing Device Status on page 313](#)

Monitoring the Secure Access as an SNMP Agent (NSM Procedure)

You can use a network management tool such as HP OpenView to monitor the Secure Access device as an SNMP agent. The Secure Access device supports SNMP (Simple Network Management Protocol) v2, implements a private MIB (management information base), and defines its own traps. To enable your network management station to process these traps, you need to download the Juniper Networks MIB file and specify the appropriate information to receive the traps.

To monitoring the Secure Access as an SNMP agent:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to monitor the Secure Access as an SNMP agent.
2. Click the **Configuration** tab, and select **System > Log/Monitoring > SNMP**. The corresponding workspace appears.
3. Add or modify settings as specified in [Table 95 on page 317](#).
4. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modification.

Table 95: Monitoring Secure Access Device as SNMP Agent Details

Option	Function	Your Action
Settings tab		
SNMP Queries	Allows you to enable SNMP queries.	Select the SNMP Queries to enable this feature.
SNMP Traps	Allows you to enable SNMP traps.	Select the SNMP Traps to enable this feature.
System Name	Specifies the system name of the Secure Access device agent.	Enter the system name.
System Location	Specifies the system location of the Secure Access device agent.	Enter the system location.
System Contact	Specifies the system contact of the Secure Access device agent.	Enter the system contact.
Community	Specifies the community string in order to query the Secure Access device, your network management station must send the Community string to the Secure Access device.	Enter the string.
Trap Settings tab		

Table 95: Monitoring Secure Access Device as SNMP Agent Details (continued)

Option	Function	Your Action
Check Frequency (seconds)	Specifies the value for check frequency trap.	Enter the value.
Log Capacity (%)	Specifies the value for log capacity trap.	Enter the value.
Users (%)	Specifies the value for users trap.	Enter the value.
Memory (%)	Specifies the value for memory trap.	Enter the value.
Swap Memory (%)	Specifies the value for swap memory trap.	Enter the value.
Disk (%)	Specifies the value for disk trap.	Enter the value.
CPU (%)	Specifies the value for CPU trap.	Enter the value.
Meeting Users (%)	Specifies the value for memory users trap.	Enter the value.
Send Traps for Critical Log Events	Allows you to send traps for critical log events.	Select the Send Traps for Critical Log Events check box to enable this feature.
Send Traps for Major Log Events	Allows you to send traps for major log events.	Select the Send Traps for Major Log Events check box to enable this feature.
SNMP Servers > Host Name/IP address	Specifies the server's host name or IP address	Enter the hostname or IP address.
SNMP Servers > Port	Specifies the port on which the server listens.	Enter the port number (typically port 162.)
SNMP Servers > Community	Specifies the community string required by the network management station.	Enter the string.



NOTE: To disable the SNMP module, you must disable the SNMP query and SNMP traps.

Related Documentation

- [Viewing Device Status on page 313](#)

PART 6

Index

- [Index on page 321](#)

Index

C

customer support.....xii
 contacting JTAC.....xii

S

support, technical See technical support

T

technical support
 contacting JTAC.....xii

